

日本国特許庁
JAPAN PATENT OFFICE

PCT/JP2005/000061

07.01.2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2004年 1月 9日
Date of Application:

出願番号 特願2004-004798
Application Number:
[ST. 10/C]: [JP2004-004798]

出願人 ソニー株式会社
Applicant(s):

2004年12月24日

特許庁長官
Commissioner,
Japan Patent Office

小川

洋

出証番号 出証特2004-3118008

【書類名】 特許願
【整理番号】 0390912004
【提出日】 平成16年 1月 9日
【あて先】 特許庁長官殿
【国際特許分類】 H04N 5/91
【発明者】
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社内
【氏名】 木谷 聰
【特許出願人】
【識別番号】 000002185
【氏名又は名称】 ソニー株式会社
【代理人】
【識別番号】 100082131
【弁理士】
【氏名又は名称】 稲本 義雄
【電話番号】 03-3369-6479
【手数料の表示】
【予納台帳番号】 032089
【納付金額】 21,000円
【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9708842

【書類名】特許請求の範囲**【請求項 1】**

データの転送を制御する転送制御手段と、
前記転送制御手段が前記データの転送を制御した回数をカウントするカウント手段と、
前記カウント手段によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断手段と、
前記第1の判断手段により前記回数が前記閾値以上になったと判断された場合、前記転送制御手段に、前記データの転送を停止するように指示を出す第1の指示手段と、
前記転送制御手段により転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成手段と、
前記転送制御手段により転送が制御される前記データを授受する他の装置から、前記初期ベクトルの供給が指示されたか否かを判断する第2の判断手段と、
前記第2の判断手段により前記初期ベクトルの供給が指示されたと判断された場合、前記生成手段に前記初期ベクトルの生成を指示するとともに、前記カウンタ手段によりカウントされている前記回数をリセットするように指示を出す第2の指示手段と
を備えることを特徴とする情報処理装置。

【請求項 2】

前記第1の指示手段による指示が出された場合、前記他の装置に対して前記データの転送が停止されたことを示すメッセージを出力する出力手段を
さらに備えることを特徴とする請求項1に記載の情報処理装置。

【請求項 3】

データの転送を制御する転送制御ステップと、
前記転送制御ステップの処理で前記データの転送が制御された回数をカウントするカウントステップと、
前記カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断ステップと、
前記第1の判断ステップの処理で前記回数が前記閾値以上になったと判断された場合、前記転送制御ステップにおける処理で、前記データの転送が停止されるように指示を出す第1の指示ステップと、
前記転送制御ステップの処理で転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、
前記転送制御ステップの処理で転送が制御される前記データを授受する他の装置から、前記初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと、
前記第2の判断ステップの処理で前記初期ベクトルの供給が指示されたと判断された場合、前記生成ステップによる処理で前記初期ベクトルが生成されるように指示するとともに、前記カウンタステップの処理によりカウントされている前記回数がリセットされるように指示を出す第2の指示ステップと
を含むことを特徴とする情報処理方法。

【請求項 4】

データの転送を制御する転送制御ステップと、
前記転送制御ステップの処理で前記データの転送が制御された回数をカウントするカウントステップと、
前記カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断ステップと、
前記第1の判断ステップの処理で前記回数が前記閾値以上になったと判断された場合、前記転送制御ステップにおける処理で、前記データの転送が停止されるように指示を出す第1の指示ステップと、
前記転送制御ステップの処理で転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、
前記転送制御ステップの処理で転送が制御される前記データを授受する他の装置から、

前記初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと、

前記第2の判断ステップの処理で前記初期ベクトルの供給が指示されたと判断された場合、前記生成ステップによる処理で前記初期ベクトルが生成されるように指示するとともに、前記カウンタステップの処理によりカウントされている前記回数がリセットされるように指示を出す第2の指示ステップと

を含む処理をコンピュータに実行させることを特徴とするプログラム。

【請求項5】

データの転送を制御する転送制御ステップと、

前記転送制御ステップの処理で前記データの転送が制御された回数をカウントするカウントステップと、

前記カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断ステップと、

前記第1の判断ステップの処理で前記回数が前記閾値以上になったと判断された場合、前記転送制御ステップにおける処理で、前記データの転送が停止されるように指示を出す第1の指示ステップと、

前記転送制御ステップの処理で転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、

前記転送制御ステップの処理で転送が制御される前記データを授受する他の装置から、前記初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと、

前記第2の判断ステップの処理で前記初期ベクトルの供給が指示されたと判断された場合、前記生成ステップによる処理で前記初期ベクトルが生成されるように指示するとともに、前記カウンタステップの処理によりカウントされている前記回数がリセットされるように指示を出す第2の指示ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【書類名】明細書

【発明の名称】情報処理装置および方法、プログラム、並びに記録媒体

【技術分野】

【0001】

本発明は、情報処理装置および方法、プログラム、並びに記録媒体に関し、特に、暗号化に関わる処理を実行する際に用いて好適な情報処理装置および方法、プログラム、並びに記録媒体に関する。

【背景技術】

【0002】

さまざまな装置で、デジタルデータを授受することが一般的になりつつあるが、デジタルデータは、不正に利用されても、その質（例えば、画質や音質）が劣化しないため、不正に利用されないための対策が必要とされる。（例えば、特許文献1参照）

【0003】

また近年普及しつつあるDVD（Digital Versatile Disc）等の記録媒体では、1枚の記録媒体（ディスク）に、例えば映画1本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となると、不正なコピーを防止して著作権者の保護を図ることが益々重要になってくる。

【0004】

そこで、例えば、DVDにビデオコンテンツを格納したDVDビデオでは、著作権保護技術として、CSS（Content Scramble System）方式が採用されている。図1は、CSS方式を用いて暗号化されたデータが記録されている記録媒体と、その記録媒体を再生する装置の構成の一例を示す図である。

【0005】

図1においては、記録媒体として、ディスク11を例に挙げて図示してある。ディスク11には、ディスク11を識別するためのディスクキー（Secured Disc Key）21、記録されているデータの所定の単位毎に設けられているタイトルキー（Encrypted Title Key）22、および、データ（Scrambled Data）23が記録されている。タイトルキー22は、例えば、ディスク11に映画が記録されているような場合、チャプター（Chapter）毎に設けられる。

【0006】

ディスクキー21とタイトルキー22は、暗号化された状態（または、容易に読み出すことが（盗用することが）できない状態）でディスク11に記録されている。また、データ23は、タイトルキー22を用いたスクランブル（Scramble）がかけられた状態でディスク11に記録されている。

【0007】

プレーヤ12は、ディスク11に記録されているキー・データを読み出すことにより、データ23の再生を行う。プレーヤ23は、復号（Decrypt）部32、復号部33、デスクランブル（DeScramble）部34、および、デコーダ（Decoder）35を有する構成とされている。また、プレーヤ12は、マスタキー（Master Key）31を管理する管理部（不図示）も有している。

【0008】

復号部32は、ディスク11から読み出されたディスクキー21を、マスタキー31を用いて復号し、その復号したディスクキー21を復号部33に供給する。復号部33には、ディスク11から読み出されたタイトルキー22も供給される。復号部33は、復号されたディスクキー21により、暗号化されているタイトルキー22を復号する。復号されたタイトルキー22は、デスクランブル部34に供給される。デスクランブル部34には、ディスク11から読み出されたデータ23も供給される。

【0009】

ディスク11から読み出され、プレーヤ12に供給されるデータ23は、所定の圧縮方式（例えば、MPEG（Moving Picture Expert Group）方式）で圧縮され、さらにタイ

トルキー22を用いたスクランブルがかけられた状態のものである。そこで、まず、デスクランブル部34は、タイトルキー22を用いて、データ23にかけられているスクランブルを解除する。

【0010】

スクランブルが解除されたデータ23は、デコーダ35に供給される。デコーダ35は、所定のデコード方式（例えば、MPEG方式）により、デスクランブル部34からのデータ23をデコードする。デコードされたデータ36は、図示されていないディスプレイなどに供給される。

【0011】

図1に示したプレーヤ12は、例えば、DVDなどのディスク11を専用に再生するような機器であるが、そのような専用のプレーヤ12に限らず、例えば、パーソナルコンピュータなどもディスク11を再生する機能を有している場合がある。

【0012】

図2は、DVDなどのディスク11をパーソナルコンピュータなどで再生する場合の構成例を示す図である。ここでは、ディスク11に記録されているデータを読み出す装置をドライブ装置51とし、ドライブ装置51により読み出されたデータを処理する装置をホスト（Host）52と記述する。図2に示したドライブ装置51やホスト52には、アプリケーションなどにより実現される機能も含まれている。

【0013】

ディスク11には、図1に示した場合と同様に、ディスクキー21、タイトルキー22、および、データ23が記録されている。ドライブ装置51は、認証（Authentication）処理部62、バス暗号化（Bus Encrypt）部62、および、バス暗号化部63を有する構成とされている。

【0014】

ホスト52は、認証処理部71、バス復号（Bus Decrypt）部72、バス復号部73、復号（Decrypt）部74、復号部75、デスクランブル部76、および、デコーダ77を有する構成とされている。また、ホスト52は、マスタキー31を管理する管理部（不図示）も有している。

【0015】

ドライブ装置51の認証処理部51とホスト52の認証処理部71は、相互認証処理を実行し、その認証処理が正常に行われたときだけ、データの授受を行う。認証処理が正常に行われると、セッションキーと称されるキーが、それぞれの認証処理部61、71において発行（共用）される。

【0016】

認証処理が正常に行われた後の時点で、ディスク11から読み出されたディスクキー21は、ドライブ装置51のバス暗号化部62により暗号化される。バス暗号化部62には、認証処理部61において発行されたセッションキーも供給される。バス暗号化部62は、読み出されたディスクキー21を、セッションキーを用いて暗号化し、ホスト71に対して出力する。

【0017】

同様に、バス暗号化部63は、ディスク11から読み出されたタイトルキー22を、認証処理部61が発行したセッションキーを用いて暗号化し、ホスト52に対して出力する。ディスク11から読み出されたデータ23は、直接的に、ドライブ装置51からホスト52に対して供給される。

【0018】

ホスト52のバス復号部72は、ドライブ装置51のバス暗号化部62から供給された暗号化されているディスクキー21を、認証処理部71により発行されたセッションキーを用いて復号する。復号されたディスクキー21は、復号部74に供給される。復号部74には、マスタキー31も供給される。復号部74は、バス復号部72から供給されたディスクキー21を、マスタキー31を用いて復号し、その復号したディスクキー21を復

号部75に供給する。

【0019】

復号部75には、バス復号部73からのタイトルキー22も供給されるが、そのタイトルキー22は、バス復号部73が、認証処理部71により発行されたセッションキーを用いて復号したものである。

【0020】

復号部75は、復号されたディスクキー21により、暗号化されているタイトルキー22を復号する。復号されたタイトルキー22は、デスクランブル部76に供給される。デスクランブル部76には、ディスク11から読み出されたデータ23も供給される。

【0021】

ディスク11から読み出されるデータ23は、所定の圧縮方式で圧縮され、さらにタイトルキー22を用いたスクランブルがかけられた状態のものである。そこでまず、デスクランブル部76は、供給されたタイトルキー22を用いて、データ23にかけられているスクランブルを解除する。

【0022】

スクランブルが解除されたデータ23は、デコーダ77に供給される。デコーダ77は、所定のデコード方式（例えば、MPEG方式）により、供給されたデータ23をデコードする。デコードされたデータ36は、図示されていないディスプレイなどに供給される。

【0023】

このように、ディスク11がセットされるドライブ装置51と、ディスク11に記録されているデータを処理するホスト52により、ディスク11に記録されているデータ23の再生の処理が実行される場合、認証処理が行われ、その認証処理が正常に行われた後に、暗号化されたキーやデータの授受が行われる。

【0024】

認証処理が行われた後に、実際のデータの授受が行われるのは、ドライブ装置51とホスト52は、所定のバス（不図示）により接続されているが、そのバスを介して授受されるデータが盗用されないようにするためである。

【0025】

ここで、認証処理部61と認証処理部71との間で行われる認証処理について、図3のフローチャートを参照して説明を加える。ステップS11において、ディスク11が、ドライブ装置51に挿入（セット）されたか否かが判断される。ステップS11において、ディスク11が、ドライブ装置51に挿入されたと判断されるまで、待機状態が維持される（ステップS11における処理が繰り返される）。

【0026】

ステップS11において、ディスク11が、ドライブ装置51に挿入されたと判断された場合、ステップS12に処理が進められる。ステップS12において、認証処理部61と認証処理部71により、相互認証の処理が実行される。この相互認証の処理が正常に終了されなければ、これ以降の処理は実行されない。

【0027】

相互認証の処理が正常に終了されると、認証処理部61と認証処理部71のそれぞれにおいて、セッションキーが生成される。このような相互認証の処理とセッションキーの発生の処理が完了したか否かが、ステップS13において判断される。ステップS13において、ステップS12における処理は完了したと判断されるまで、ステップS12の処理が繰り返され、完了したと判断された場合、ステップS14に処理が進められる。

【0028】

ステップS14において、スクランブルされたデータの授受（ドライブ装置51からの出力）が許可された状態に設定される。この場合、スクランブルされたデータとは、データ23（図2）のことであり、このデータ23のドライブ装置51からホスト52への出力が許可された状態に設定される。

【0029】

“許可された状態”ということについて説明を加える。データ23の読み出しは、ホスト52からの指示に基づいてドライブ装置51が行う。許可される前の状態において、ドライブ装置51は、仮にホスト52からデータ23の読み出し（出力）の指示を受けたとしても、エラーを返すだけで、データ23の出力は行わない。

【0030】

許可された後の状態においては、ホスト52からデータ23の読み出した指示されれば、ドライブ装置51は、ディスク11からデータ23を読み出し、ホスト52に対して出力を行う。

【0031】

このような状態に設定されると、ディスク11がドライブ装置51から排出されるなどの割り込み処理が発生しない限り、スクランブルされたデータ23の再生の処理が繰り返し行われる。

【0032】

スクランブルされたデータ23の出力が許可された状態にされると、ステップS15において、ディスク11がドライブ装置51から排出された否かの判断が継続的に行われる。そして、ステップS15において、ディスク11がドライブ装置51から排出されたと判断されると、ステップS11に処理が戻され、それ以降の処理が繰り返される。

【0033】

なお、ドライブがリセットされた場合や、電源がオフの状態にされた場合も、再生の処理が終了され、必要に応じ、ステップS11に処理が戻され、それ以降の処理が繰り返される。

【0034】

このようにして、ドライブ装置51とホスト52との間で認証処理が正常に終了されると、ドライブ装置51側では、ディスク11が排出されるまで、その挿入されているディスク11からデータ23を読み出し、その読み出したデータ23をホスト52に出力するという処理を、ホスト52からの指示がある限り継続的に行なわれる。

【0035】

ここで、バス暗号化部62などの暗号化部において行われる公知の暗号化技術について説明を加える。暗号化の方式は、さまざまなもののが提案されている。ここでは、CBC（Cipher Block Chaining）方式を例に挙げて、暗号化（復号）の方式について説明する。

【0036】

暗号化の一方式であるCBC方式は、ブロック連鎖のための一つの技法であり、排他的論理和演算により、平文の現在のブロックに暗号文の前のブロックを付加して、暗号文の各ブロックを作成する方式である。図4は、CBC方式を用い暗号化を行う回路の一例を示す図である。

【0037】

暗号化すべきデータは、所定の単位（例えば、ブロック暗号方式としてAES（Advanced Encryption Standard）を用いた場合は16バイト）毎にブロック化される。そして、第1のブロックは、排他的論理和回路101-1に供給され、第1のブロックに続く第2のブロックは、排他的論理和回路101-2に供給され、第2のブロックに続く第3のブロックは、排他的論理和回路101-3に供給されというように、所定の段数（ここでは、N段とする）だけ設けられた排他的論理和回路101-1乃至101-Nに順次、ブロック化された平文のデータが入力される。

【0038】

排他的論理和回路101-1から出力された第1のブロックは、暗号化部102-1に供給される。暗号化部102-1は、鍵Ekで供給された第1のブロックを暗号化する。このようにして、第1のブロックは暗号化される。

【0039】

暗号化部102-1から出力された暗号化された第1のブロックは、排他的論理和回路

101-2 にも供給され、第2のブロックとの間で排他的論理和が演算される。その結果は、暗号化部102-2 に供給され、同じく鍵E_k で暗号化される。

【0040】

このように、CBC方式における暗号化は、1つ前で暗号化したブロックと暗号化対象の現在の平文のブロックとの排他的論理和が演算されてから、そのブロックに対して所定の暗号化鍵での暗号化が行なわれるようになっている。結果の暗号文は次のブロックとの排他的論理和の演算に使われることになる。このように前のブロックと次々に連鎖されることにより暗号文が生成される。

【0041】

第2のブロック以降は、前のブロックとの排他的論理和が演算されるが、第1のブロックは、前のブロックが存在しないため、前のブロックとの排他的論理和を演算することができない。そこで、第1のブロックに対しては、初期ベクトル（IV：Initializing Vector）を与えて排他的論理和を演算するように構成される。

【0042】

次に、CBC方式を用い復号を行う回路（例えば、バス復号部72（図2））について、図5を参照して説明する。

【0043】

上述したようにして暗号化されたデータは、所定の単位（例えば、ブロック暗号方式としてAES（Advanced Encryption Standard）を用いた場合は16バイト）毎にブロック化されている。ブロック化されているデータの内、第1のブロックは、復号部122-1に供給され、第1のブロックに続く第2のブロックは、復号部122-2に供給され、第2のブロックに続く第3のブロックは、復号部122-3に供給されというように、所定の段数（ここでは、N段とする）だけ設けられた復号部122-1乃至122-Nに順次、暗号化されたブロック単位のデータが入力される。

【0044】

各復号部122-1乃至122-Nは、入力されたデータを鍵D_k で復号する。各復号部122-1乃至122-Nから出力されたデータは、対応する排他的論理和回路121部1-1乃至121-Nに供給される。排他的論理和回路121-2乃至121-Nには、前の段の復号部122-1乃至122-N-1に供給されるデータも供給される。

【0045】

このように、CBC方式の復号は、1つ前の暗号化されているブロックと復号対象の現在の復号されたブロックとの排他的論理和が演算されることにより、最終的な復号が行われる。

【0046】

第2のブロック以降は、前のブロックとの排他的論理和が演算されるが、第1のブロックは、前のブロックが存在しないため、前のブロックとの排他的論理和を演算することができない。そこで、第1のブロックに対しては、初期ベクトルIVを与えて、排他的論理和が演算される構成とされている。

【0047】

このようにして、暗号化、復号が行われている。

【特許文献1】特許第3252706号明細書

【発明の開示】

【発明が解決しようとする課題】

【0048】

ところで、図2に示したように、ドライブ装置51とホスト52によりディスク11に記録されているデータ23の再生の処理が実行される場合、図3のフローチャートを参照して説明したように、ドライブ装置51とホスト52における相互認証の処理が正常に終了されると、ドライブ装置51からのデータ23の出力が許可された状態にされる。

【0049】

ここで、図6を参照して説明するに、ホスト52側でアプリケーションAが起動され、

そのアプリケーションAにより、認証処理部71で行う認証処理が実行される場合を考える。アプリケーションAによるドライブ装置51との認証処理が正常に実行されると、ドライブ装置51からディスク11からデータ23が読み出され、出力されるといった処理が許可された状態にされる。

【0050】

許可された状態のときに、ディスク11がドライブ装置51から排出されるなどの状況が発生しない限り、ドライブ装置51からデータ23が出力されるといった処理が許可された状態が維持される。そのような許可が維持されている状態のときに、アプリケーションBがホスト52側で起動されたとする。そして、アプリケーションAにかわり、アプリケーションBにより、データ23の読み出しの指示などの処理が開始されたとする。

【0051】

ドライブ装置51とアプリケーションBは、認証処理を行っていないにもかかわらず、ドライブ装置51は、データ23の出力が許可された状態に維持されているため、ドライブ装置51からホスト52（アプリケーションB）に対して、データ23は出力されてしまう。その結果、例えば、ホスト52が有するHDD（Hard Disc Drive）141にデータ23が記憶されるといった処理が、アプリケーションBにより実行される可能性がある。

【0052】

このHDD141に対するデータ23の記憶が不正な処理であっても、ドライブ装置51は、アプリケーションBの指示に基づき、データ23を出力してしまう。よって、このような不正を防ぐことができないといった課題があった。

【0053】

また、HDD141に記憶されたデータ23は、スクランブルがかけられた状態であるため、そのままでは再生することができないが、スクランブルを解除するアプリケーションなども存在しているため、実質的には、HDD141にデータ23が記憶された時点で、不正に利用されてしまうことを防ぐことができないといった課題があった。

【0054】

このように、一旦、正常に認証処理が行われ、ドライブ装置51側でデータ23の出力が許可された状態にされると、データ23が盗用されてしまう可能性があるといった課題があった。

【0055】

図7を参照し、他のデータの盗用について説明する。ドライブ装置51とホスト52は、所定のバスにより接続され、そのバスを介してデータ23の授受を行うように構成されている。図6を参照して説明した場合と同様に、アプリケーションAにより、ドライブ装置51との認証処理が行われる。そして、その認証処理が正常に行われると、ドライブ装置51からデータ23を出力するといった処理を実行することが許可された状態とされる。

【0056】

バス上を授受されるデータをモニタする機能をホスト52が有していると、そのモニタ151により、バス上で授受されているデータ23をモニタする（取得する）ことが可能である。換言すれば、ドライブ装置51から出力されたデータ23は、アプリケーションAとモニタ151に供給されるといった状態にすることが可能である。

【0057】

そのため、ホスト52側で、モニタ151により取得されたデータ23を、HDD141に記憶させるといった処理を実行することも可能となる。よって、このようにしてデータ23が盗用されてしまう可能性もある。

【0058】

このように、バス上を授受されるデータが、モニタ機能により盗用されてしまう可能性があるといった課題があった。

【0059】

バス上のデータが盗用されてしまうようなことを防ぐために、バスを介して授受されるデータ 23 を暗号化する方法も提案されている。図 8 を参照して説明する。ドライブ装置 51 側からホスト 52 に出力されるデータを転送データ 171 と記述する。

【0060】

転送データ 171 は、2048 バイト (2K バイト) のデータパケット (data Packet) とされる。上述したように、ドライブ装置 51 とホスト 52 は、所定のバスで接続されているわけだが、そのバスをコントロールするバスインターフェース 183 は、所定の単位量のデータを取り扱うように規定されている。その単位量は、例えば、ATAPI (AT Attachment with Packet Interface) をバスインターフェース 183 として用いた場合、2048 バイトと規定されている。

【0061】

そこで、転送データ 171 を 2048 バイトで構成されるデータパケットとした場合、図 8 に示すように、1 パケットは、16 バイトの初期ベクトル IV と 2032 バイトのデータから構成される。このようなデータパケットのうち、2032 バイトのデータ部分が、暗号化部 181 により暗号化される。暗号化部 181 は、図 8 には図示していないが、認証処理部 181 (図 2) により発行されるセッションキー Ks を用いて暗号化を行う。

【0062】

暗号化部 181 は、例えば、CBC 方式を用いて暗号化を行う。CBC 方式に基づいて暗号化を行う場合、暗号化部 181 の内部構成例は、図 4 に示したようになる。図 4 を参考して説明したように、暗号化部 181 は、初期ベクトル IV も用いて暗号化を行う。なわち、暗号化部 181 は、転送データ 171 のデータパケットの内、2038 バイトのデータ部分を、同じくデータパケット内に含まれる 16 バイトの初期ベクトル IV と、認証処理部 181 により発行されるセッションキー Ks を用いて暗号化を行う。

【0063】

暗号化部 181 により暗号化されたデータパケットも、2048 バイトのデータである。よって、その暗号化されたデータパケットは、バスインターフェース 183 により取り扱うことができる。データ部分が暗号化されたデータパケットは、ホスト 52 側の復号部 182 に供給される。復号部 182 は、供給されたデータパケットに含まれる初期ベクトル IV と、認証処理部 71 (図 2) により発行されるセッションキー Ks を用いて、暗号化されているデータの復号を行う。

【0064】

このようにして、ホスト 52 側は、暗号化されたデータを受信するが、そのデータと共に供給される初期ベクトル IV を用いて復号することができるため、ホスト 52 側において、ドライブ装置 51 側から出力されたデータを再生することができる。

【0065】

このように、バスインターフェース 183 上で授受されるデータを、暗号化されたデータとすることにより、仮に、バスインターフェース 183 を介して授受されるデータが盗聴されても、暗号化を解くことができなければ、盗用されることがなく、結果として、データが不正に利用されるような不都合が発生するようなことを防ぐことが可能となる。しかしながら、以下のような問題点がある。

【0066】

再度、図 8 を参照するに、初期ベクトル IV は、転送データ 171 に含まれている。転送データ 171 に初期ベクトル IV を含ませる場合、ディスク 11 に、他のデータと共に書き込まれている。よって、初期ベクトル IV をランダムに変化させることができない (書き込まれている初期ベクトル IV をそのまま用いなくてはならず、変化させることができない) といった問題点があった。

【0067】

また、ディスク 11 に初期ベクトル IV が書き込まれているのではなく、ドライブ装置 51 側でランダムに初期ベクトル IV を発生させ、その初期ベクトル IV を転送データ 171 内に含ませるようにすることも考えられ。しかしながら、転送データ 171 に初期ベクトル IV を含ませることも考えられる。

クトルIVを含ませる場合、暗号化されるデータと区別するために、例えば、ヘッダなどを付けなくてはならないなどの条件がある。

【0068】

そのような条件があるために、ドライブ装置51側で、ランダムに初期ベクトルIVを発生させるようにしても、ランダムに変化させることに対する制限があり、結果的には、ランダムに初期ベクトルIVを発生させるということに対してそのランダム性を保証することができない（固定パターンになってしまう）といった問題があった。

【0069】

初期ベクトルIVをランダムに変化させることができない場合、換言すれば、初期ベクトルIVとして固定パターンが用いられるようにすると、以下のような問題が発生する可能性がある。

【0070】

例えば、電子メールを例に挙げて考える。電子メールの書式には、宛先、送信元、件名、本文といったような一連のパターンがある。そのようなパターンがあるようなデータ（平文）を暗号化した場合、暗号化されたデータ自体もパターンがあるデータとなってしまう。第3者（攻撃者）が、そのようなパターンに注目することにより、暗号文から平文の一部を解読することが可能である。

【0071】

また、音楽データなどで、その音楽データを繰り返し再生するような場合、結果として同じ平文を同じように暗号化することになり、暗号化されたデータ自体も同じ結果となる。そのため、上述した場合と同様に、暗号文から平文を解読することが可能である。

【0072】

そこで、パターンがあるような平文（同一のデータを複数回暗号化するような場合）でも、暗号化されたデータ（暗号文）にパターンがないようにするために、最初のブロックに初期ベクトルIVを加えるようにする。初期ベクトルIVを加えて暗号化を実行することにより、平文のブロックに同じパターンがあっても暗号文には同じパターンが発生しないので、暗号解読を困難にさせることができるのである。また、単一の鍵で大量のデータを暗号化した場合に暗号鍵が予測しやすくなる、という解読行為を、初期ベクトルIVを加えて暗号化を行うようにすることで防止することができるという効果もある。

【0073】

このような理由で最初のブロックに初期ベクトルIVが加えられ、その後の暗号化が行われるように構成されている場合が多い。

【0074】

そして、初期ベクトルIVを適当に更新させることで、平文のデータが特別なパターンのデータであることを特定させることを困難とし、データのすり替え、データの改竄行為を防止することができるとされている。（参考文献：NIST Special Publication 800-38A 2001 Edition, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, APPENDIX C Generation of Counter Blocks）

【0075】

よって、同じ初期ベクトルIVが繰り返し用いられると、結果として、初期ベクトルIVを適当に更新させることで、平文のデータが特別なパターンのデータであることを特定させることを困難とし、データのすり替え、データの改竄行為を防止することができないといった課題があった。

【0076】

また、上述したように、初期ベクトルIVは、更新される方が好ましいといった課題があった。

【0077】

そこで、初期ベクトルIVを更新できるようにした場合、図9に示すようなデータの授受の方法が考えられる。すなわち、図9に示した例では、転送データ191は、2048バイトのデータから構成され、そのデータに、16バイトの初期ベクトルIVが付加され

る。そして、初期ベクトルIVが付加された結果、2064バイトにされたデータが、バスインターフェース183を介して授受される。

【0078】

初期ベクトルIVを転送データ191に付加する構成とすることにより（転送データ191に初期ベクトルIVを予め含めるような構成としないことにより）、初期ベクトルIVを、ドライブ装置51側でランダムに発生し、そのランダムに発生された初期ベクトルIVを付加させることができるようになる。

【0079】

しかしながら、このようにして初期ベクトルIVをデータに付加することは、例えば2048バイト単位のPC Drive Interfaceに、2064バイト(IV=16バイトの場合)という特殊なセクタサイズを持ち込むことになり、標準的なフォーマットから外れてしまうこととなる。そのために、共通の ATAPI Device Driver を利用できない、UDF (Universal Data Format) で扱うことのできるセクタサイズである2048バイトや4096バイトに当たはまらないためUDF FS Driverを利用できないなど、パーソナルコンピュータにおける環境との相性がよくないといった課題があった。

【0080】

相性が良くないといったことを解決するためには、ハードウェア的に、ソフトウェア的にも特殊なものに変えなくてはならないなど、コスト的に割高になり、互換性を取りづらい、処理的に手間がかかるといった課題もあった。

【0081】

本発明はこのような状況に鑑みてなされたものであり、認証処理が正常に終了し、ドライブ装置側からデータが出力されることが許可された状態にされた後においても、その許可状態を解除できるようにし、データの盗用を防ぐことを目的とする。また、汎用なバスを用いた場合においても、初期ベクトルIVを更新できるようにし、そのバス上で授受されるデータが盗用されないようなセキュリティを高めることを目的とする。

【課題を解決するための手段】

【0082】

本発明の情報処理装置は、データの転送を制御する転送制御手段と、転送制御手段がデータの転送を制御した回数をカウントするカウント手段と、カウント手段によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断手段と、第1の判断手段により回数が閾値以上になったと判断された場合、転送制御手段に、データの転送を停止するように指示を出す第1の指示手段と、転送制御手段により転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成手段と、転送制御手段により転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第2の判断手段と、第2の判断手段により初期ベクトルの供給が指示されたと判断された場合、生成手段に初期ベクトルの生成を指示するとともに、カウンタ手段によりカウントされている回数をリセットするように指示を出す第2の指示手段とを備えることを特徴とする。

【0083】

前記第1の指示手段による指示が出された場合、他の装置に対してデータの転送が停止されたことを示すメッセージを出力する出力手段をさらに備えるようにすることができる。

【0084】

本発明の情報処理方法は、データの転送を制御する転送制御ステップと、転送制御ステップの処理でデータの転送が制御された回数をカウントするカウントステップと、カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断ステップと、第1の判断ステップの処理で回数が閾値以上になったと判断された場合、転送制御ステップにおける処理で、データの転送が停止されるように指示を出す第1の指示ステップと、転送制御ステップの処理で転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、転送制御ステップの処理

で転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと、第2の判断ステップの処理で初期ベクトルの供給が指示されたと判断された場合、生成ステップによる処理で初期ベクトルが生成されるよう指示するとともに、カウンタステップの処理によりカウントされている回数がリセットされるように指示を出す第2の指示ステップとを含むことを特徴とする。

【0085】

本発明のプログラムは、データの転送を制御する転送制御ステップと、転送制御ステップの処理でデータの転送が制御された回数をカウントするカウントステップと、カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断ステップと、第1の判断ステップの処理で回数が閾値以上になったと判断された場合、転送制御ステップにおける処理で、データの転送が停止されるように指示を出す第1の指示ステップと、転送制御ステップの処理で転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、転送制御ステップの処理で転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと、第2の判断ステップの処理で初期ベクトルの供給が指示されたと判断された場合、生成ステップによる処理で初期ベクトルが生成されるよう指示するとともに、カウンタステップの処理によりカウントされている回数がリセットされるように指示を出す第2の指示ステップとを含む処理をコンピュータに実行させることを特徴とする。

【0086】

本発明の記録媒体のプログラムは、データの転送を制御する転送制御ステップと、転送制御ステップの処理でデータの転送が制御された回数をカウントするカウントステップと、カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断ステップと、第1の判断ステップの処理で回数が閾値以上になったと判断された場合、転送制御ステップにおける処理で、データの転送が停止されるように指示を出す第1の指示ステップと、転送制御ステップの処理で転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、転送制御ステップの処理で転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと、第2の判断ステップの処理で初期ベクトルの供給が指示されたと判断された場合、生成ステップによる処理で初期ベクトルが生成されるよう指示するとともに、カウンタステップの処理によりカウントされている回数がリセットされるように指示を出す第2の指示ステップとを含むことを特徴とする。

【0087】

本発明の情報処理装置および方法、並びにプログラムにおいては、初期ベクトルの供給の指示が定期的に行われなければ、データの授受が停止される。

【発明の効果】

【0088】

本発明によれば、装置間での転送路上におけるセキュリティを高めることが可能となる。

。

【0089】

また、本発明によれば、記録媒体を扱う装置とその装置からのデータを扱う他の装置との間で認証処理が行われた後、記録媒体を扱う装置側で、記録媒体から読み出したデータを他の装置に出力することが許可された状態にされても、その状態を解除（更新）することができる。もって、一旦、他の装置へのデータの出力が許可された状態であっても、その後の不正なアクセスによるデータの流出を防ぐことが可能となる。

【0090】

また、本発明によれば、暗号化の際に用いられる初期ベクトルをランダムに更新することができ、同一のデータを暗号化しても、同一の暗号文が生成されるようなことを防ぐことが可能となる。もってデータのすり替え、データの改竄行為などの不正な処理を防止することができる。

【0091】

また、本発明によれば、初期ベクトルを更新するようにしても、汎用のバスインターフェースおよびOS(Operating System)で標準的に用意されたUDF FS Driverを利用できる。もって、初期ベクトルを更新できるようにするために、装置間の環境を変更しなくてはならないといったような不都合が発生するようなことを防ぐことができる。

【発明を実施するための最良の形態】

【0092】

以下に本発明の最良の形態を説明するが、開示される発明と実施の形態との対応関係を例示すると、次のようになる。明細書中には記載されているが、発明に対応するものとして、ここには記載されていない実施の形態があったとしても、そのことは、その実施の形態が、その発明に対応するものではないことを意味するものではない。逆に、実施の形態が発明に対応するものとしてここに記載されていたとしても、そのことは、その実施の形態が、その発明以外の発明には対応しないものであることを意味するものでもない。

【0093】

さらに、この記載は、明細書に記載されている発明の全てを意味するものではない。換言すれば、この記載は、明細書に記載されている発明であって、この出願では請求されていない発明の存在、すなわち、将来、分割出願されたり、補正により出現し、追加される発明の存在を否定するものではない。

【0094】

本発明を適用した情報処理装置は、データの転送を制御する転送制御手段（例えば、図13のステップS46の処理を実行する図10のセクタ転送制御部313）と、転送制御手段がデータの転送を制御した回数をカウントするカウント手段（例えば、図13のステップS47の処理を実行する図10のセクタ転送カウンタ314）と、カウント手段によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断手段（例えば、図13のステップS45の処理を実行する図10のセクタ転送カウンタ314）と、第1の判断手段により回数が閾値以上になったと判断された場合、転送制御手段に、データの転送を停止するように指示を出す第1の指示手段（例えば、図10のセクタ転送カウンタ314）と、転送制御手段により転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成手段（例えば、図13のステップS41の処理を実行する図10の乱数発生部315）と、転送制御手段により転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第2の判断手段（例えば、図13のステップS40の処理を実行する図10のコマンド処理部317）と、第2の判断手段により初期ベクトルの供給が指示されたと判断された場合、生成手段に初期ベクトルの生成を指示するとともに、カウンタ手段によりカウントされている回数をリセットするように指示を出す第2の指示手段（例えば、図13のステップS42の処理を実行する図10の乱数発生部315）とを少なくとも備える。

【0095】

前記第1の指示手段による指示が出された場合、他の装置に対してデータの転送が停止されたことを示すメッセージを出力する出力手段（例えば、図13のステップS48の処理を実行する図10のメッセージ伝達部316）をさらに備える。

【0096】

以下に、本発明の実施の形態について図面を参照して説明する。

【0097】

図10は、本発明を適用したシステムの一実施の形態の構成を示す図である。

【0098】

図10に示したシステムは、所定の記録媒体に記録されたデータを再生する（読み出す）システムの構成例を示している。図10に示したシステムは、データを供給するドライバ装置301と、データの供給を受けるホスト302から構成されている。

【0099】

ディスク303は、例えば、CD-ROM（Compact Disc-ROM）、CD-R（Compact Disc-Reco

rdable)、CD-RW (Compact Disc-ReWritable)、DVD-ROM (Digital Versatile Disc-RO M)、DVD-R (Digital Versatile Disc-Recordable)、DVD-RW (Digital Versatile Disc-Rerecordable)、DVD+R (DVD+Recordable)、DVD+RW (DVD+ReWritable)、DVD-RAM (Digital Versatile Disk-Random Access Memory)、Blu-Ray Discなどである。また、本発明の適用範囲はこれらの記録媒体に限定されるものではなく、他の形態（記録方式、形状など）の記録媒体を扱うシステムにも適用可能である。

【0100】

ドライブ装置301とホスト302は、所定のインターフェースによりデータの授受が行えるように接続されている。所定のインターフェースとしては、例えば、ATAPI (ATA Attachment with Packet Interface) を用いることができる。ATAPIは、IDE (Integrated Drive Electronics) や、ATA (AT Attachment) インターフェースにCD-ROMドライブなどハードディスク以外の周辺機器を接続するためのデータ転送方式に従ったインターフェースであり、例えばSCSIから流用したコマンドをパケット化してIDEインターフェースに渡すことによって周辺機器の制御を可能とする。同様のコマンドパケットはUSB (Universal Serial Bus) や IEEE1394などの物理インターフェースへも適用可能である。

【0101】

ドライブ装置301は、認証処理部311、暗号化部312、セクタ転送制御部313、セクタ転送カウンタ314、乱数発生部315、メッセージ伝達部316、コマンド処理部317、および、アクセス処理部318を含む構成とされている。

【0102】

ホスト302は、認証処理部321、復号部322を含む構成とされている。

【0103】

ドライブ装置301の認証処理部311とホスト302の認証処理部321により、相互認証に関わる処理が実行される。

【0104】

暗号化部312には、アクセス処理部318による処理により、ディスク303から読み出されたセクタデータ351と、認証処理部311からセッションキーKsが供給される。また、暗号化部312には、乱数発生部315により発生された乱数が、初期ベクトルIVとして供給される。

【0105】

なお、乱数発生部315により発生された乱数を、そのまま初期ベクトルIVとして用いても良いが、乱数と他のデータ（例えば、ディスク303から読み出されるPSN (Physical Sector Number) など）が用いられて生成されるものを初期ベクトルIVとして用いられるようにしても良く、そのような処理を実行する部分を、ドライブ装置301内に設けるようにしても良い。

【0106】

暗号化部313は、供給されたセクタデータ351をセッションキーKsと初期ベクトルIVを用いて暗号化し、セクタ転送制御部313に供給する。セクタ転送制御部313は、暗号化されたセクタデータ351を、ホスト303の復号部322に対して供給する。よって、ドライブ装置301からホスト303に供給されるデータは、暗号化されたセクタデータ351である。

【0107】

暗号化部312からは、セクタ転送カウンタ314にもデータが出力される。セクタ転送カウンタ314は、ホスト302に対して出力されたセクタデータ（暗号化部312から出力されたセクタデータ351）の数をカウントするように構成されている。換言すれば、セクタ転送カウンタ314は、セクタ転送制御部313がセクタデータの転送を制御した回数をカウントする。

【0108】

また、セクタ転送カウンタ314は、予め設定されたカウント数の最大値（N_{max}とす

る)を管理しており、カウントしているセクタ数(カウンタ値N)が、その最大値を超えないか否かを常に監視している。

【0109】

セクタ転送カウンタ314は、 $N \geq N_{max}$ になった場合、セクタ転送制御部313に対して、ホスト302へのセクタデータ351の出力を停止するように指示を出す。このよして、ホスト302へのセクタデータ351の出力を停止するように指示を出す。このよして、ホスト302へのセクタデータ351の出力を停止するように指示を出す。このよして、ホスト302へのセクタデータ351の出力を停止するように指示を出す。

【0110】

セクタ転送制御部313は、セクタ転送カウンタ314からセクタデータ351の出力の停止の指示を受けた場合、メッセージ伝達部316に対して、メッセージ362(この場合、エラーメッセージ)をホスト302に対して出力するように指示を出す。

【0111】

一方、ホスト303の復号部322は、ドライブ装置301からインターフェースを介して暗号化されたセクタデータ351の供給をうける。復号部322は、ドライブ装置301から、セクタデータ351とは別の経路(詳細は図11を参照して後述する)で、乱数発生部315により発生された初期ベクトルIVも供給される。

【0112】

復号部322は、認証処理部331から供給されるセッションキーKsと、ドライブ装置301から供給された初期ベクトルIVを用いて復号処理を実行し、セクタデータ361を生成する。

【0113】

ホスト302からは、コマンドパケット363が必要に応じて、ドライブ装置301に対して供給される。このコマンドパケット363は、例えば、ディスク303からデータの読み出しを指示するリードコマンド(Read command)、ディスク303へのデータの書き込みを指示するライトコマンド(Write command)、初期ベクトルIVの発行を指示するレポートキーコマンド(Report Key command)などがある。

【0114】

図11を参照して、セクタデータ351が授受される経路と、その他のデータが授受される経路について説明する。PC driver391は、例えば、初期ベクトルIVの生成、暗号化セクタデータの作成、転送セクタデータの作成などを制御するドライバーである。PC driver391からのデータは、Optical Disc driver392に渡される。

【0115】

Optical Disc driver392は、光ディスク(Optical Disc)の読み出しや書き込みを制御するドライバーである。光ディスクがDVDなどの記録媒体である場合、その光ディスクに書き込まれているデータ(ファイル)は、UDF(Universal Data Format)に準拠したるものとされている。よって、Optical Disc driver392により読み出された(制御された)データ(ファイル)は、UDF FS driver393の制御により、Optical Disc file reader394を介して、Video/Audio Playback function395に渡される。

【0116】

Video/Audio Playback function395は、例えば、転送セクタデータの取得、初期ベクトルIVの取得、暗号化セクタデータの復号を制御する。

【0117】

このように、セクタデータなどの映像や音声に関わるデータは、UDF FS driver393を介して授受されるが、その他の、例えば、初期ベクトルIVやその初期ベクトルIVを発行させるためのコマンドなどのデータは、UDF FS driver393を介さずに授受される。このUDF FS driver393を介さずに行われるデータの授受の経路は、Microsoft Windows(登録商標)においてはSCSI PASS Throughなどと称されている。

【0118】

図10において、ドライブ装置301とホスト302との間に図示されている線のうち

、太線で示した経路が、UDF FS driver 393を介してデータの授受が行われる経路（以下、適宜、UDF経路と称する）を示し、細線で示した経路が、その他のデータの授受が行われる経路（SCSI PASS Through、以下、適宜、パス経路と称する）を示すとする。

【0119】

図10に示したように、セクタ転送制御部313から復号部322への経路がUDF経路である。認証処理部311と認証処理部321との間で行われる認証処理に必要とされるデータの授受は、パス経路を介して行われる。また、メッセージ伝達部316から出力されるメッセージ362は、パス経路を介して授受される。また、初期ベクトルIVも、パス経路を介して授受される。

【0120】

UDF FS driver 393は、2048バイトのデータ、または、2048バイトの整数倍のデータ容量のデータを取り扱う。よって、UDF経路を介して授受されるデータは、2048バイトまたはその倍数のデータしか通すことができない。

【0121】

これに対し、パス経路は、基本的にデータの容量にかかわらず授受することが可能である。よって、16バイトで構成される初期ベクトルIVなどを授受をするのに適した経路である。

【0122】

図10に示した構成のドライブ装置301の動作について、図12と図13のフローチャートを参照して説明する。ステップS31において、ドライブ装置301にディスク303が、挿入されたか否かが判断される。ステップS31において、ドライブ装置301にディスク303が挿入されたと判断された場合、ステップS32に処理が進められ、ホスト302において所定のアプリケーションが起動されたか否かが判断される。

【0123】

所定のアプリケーションとは、ドライブ装置301に挿入されたディスク303からデータを読み出す、または、書き込むために必要とされるアプリケーションである。

【0124】

ステップS32において、ホスト302において所定のアプリケーションが起動されたと判断された場合、ステップS33に処理が進められる。ステップS33において、ドライブ装置301とホスト302との間で相互認証処理が実行され、セッションキーKsがドライブ装置301とホスト302で、それぞれ生成（共用）される。ステップS34において、セッションキーKsの生成が完了したか否かが判断される。セッションキーKsの生成が完了されるまで、ステップS33とステップS34の処理が繰り返される。

【0125】

そして、ステップS34において、セッションキーKsの生成が完了したと判断されると、ステップS35に処理が進められ、ドライブ装置301のセクタ転送カウンタ314のカウンタ値Nが、予め設定されているカウンタ値Nの最大値である値N_{max}に設定される（N=N_{max}に設定される）。

【0126】

このように、N=N_{max}に設定されると、セクタ転送カウンタ314の指示により、セクタ転送制御部313からホスト302へのデータの出力が許可されない状態に設定される。

【0127】

ステップS36において、ホスト302から初期ベクトルIVの転送要求があつたか否かが判断される。この判断は、コマンド処理部317が、ホスト302側から、コマンドパケット363を受信したか否かを判断し、かつ、受信したコマンドパケット363が、初期ベクトルIVの転送要求を示すものであるか否かを判断することにより行われる。

【0128】

ステップS36において、初期ベクトルIVの転送要求があつたと判断されるまで、ステップS36の処理が繰り返される。そして、ステップS36において、初期ベクトルIV

Vの転送要求があったと判断された場合、ステップ37に処理が進められ、初期ベクトルIVの生成が行われる。

【0129】

コマンド処理部317は、ホスト302からのコマンドパケット363を受信し、そのコマンドパケット363を解析することにより、初期ベクトルIVの転送要求であると判断すると、そのことを、乱数発生部315に知らせる。そのような知らせを受けた乱数発生部315は、ステップS37の処理として、初期ベクトルIVを生成する。

【0130】

乱数発生部315は乱数を発生するが、その乱数が、そのまま初期ベクトルIVとされる。または、発生された乱数と所定の情報（例えば、初期ベクトルIVの転送要求を指示するコマンドパケット363に含まれる情報）などを用い、排他的論理和を算出するなどの処理が実行されることにより、初期ベクトルIVが発生されるようにしても良い。

【0131】

乱数発生部315は、初期ベクトルIVを生成すると共に、セクタ転送カウンタ314に対して、カウンタ数Nを0に設定し直すように指示を出す。このような指示を受け取ったセクタ転送カウンタ314は、ステップS38の処理として、カウンタ値Nを0に設定し直す。このようにセクタ転送カウンタ314のカウンタ値Nが、0に設定されると、セクタ転送制御部313からのデータの出力が許可された状態に変更される。

【0132】

乱数発生部315により生成された初期ベクトルIVは、ステップS39において、ホスト302に供給される。この初期ベクトルIVの供給（転送）は、バス経路を介して行われるため、例えば、初期ベクトルIVが16バイトで構成される場合であっても、その16バイトの初期ベクトルIVをドライブ装置301とホスト302側で授受することが可能である。

【0133】

ステップS33乃至S39の処理のうち、初期ベクトルIVの授受に関わる処理について、図14を参照して説明を加える。

【0134】

ホスト302は、ステップS101において、ドライブ装置301は、ステップS111において、それぞれ相互認証（Authentication）を行う。この相互認証が正常に行われた場合のみ、次のステップに処理が進められる。また、この相互認証の結果、ドライブ装置301の認証処理部311とホスト302の認証処理部321との、それぞれにおいてセッションキーKsが生成される（共有される）ことになる。

【0135】

ホスト302は、ステップS102において、コマンドパケット363を生成し、ドライブ装置301に対して出力する。ステップS102において生成され、出力されるコマンドパケット363は、REPORT KEY commandであり、このREPORT KEY commandは、ここでは、初期ベクトルIVの転送を要求するものであるとする。

【0136】

そのようなREPORT KEY commandを、ステップS112の処理として受信したドライブ装置301は、ステップS113において、初期ベクトルIVを生成する。生成された初期ベクトルIVは、ステップS114において、ドライブ装置301からホスト302に対して出力される。この出力される初期ベクトルIVは、そのままホスト302側に出力される。

【0137】

このようにしてドライブ装置301から出力された初期ベクトルIVを、ホスト303は、ステップS103において受信する。

【0138】

このように、ドライブ装置301からホスト302に転送される初期ベクトルIVを、暗号化などの処理を施さずに、そのまま転送されるようにしても良いが、暗号化が施され

た状態で転送されるようにしてももちろん良い。

【0143】

初期ベクトルIVは、乱数発生部315により乱数を用いて発生されるため、ランダムに変化される値である。また、初期ベクトルIVは、セッションキーKsと異なり、秘匿する必要性は低いと考えられる。このようなことを考慮し、図14を参照して説明したように、転送される初期ベクトルIVは、そのまま転送されるようにしても良い。

【0144】

しかしながら、初期ベクトルIVは、予測不可能であることが好ましいという条件がある。その条件を満たすために、転送される初期ベクトルIVを暗号化し、より安全性を高めるようにしてももちろん良い。

【0145】

より安全性を高めて初期ベクトルIVが転送されるようにした場合、図15に示すように処理が行われる。ホスト302側で行われるステップS131乃至S133における処理は、基本的に、図14におけるステップS101乃至S103と同様に行われるが、ステップS103において受信される初期ベクトルIVは、暗号化されているため、受信された後に、復号という処理が実行される点が異なる。

【0146】

ドライブ装置301側で行われるステップS141乃至S144における処理も、基本的に、図14におけるステップS111乃至S114と同様であるが、ステップS143において、初期ベクトルIVが生成されたあと、その初期ベクトルIVが、セッションキーKsが用いられて暗号化され、その暗号化された初期ベクトルIV(E[Ks, IV])が、ステップS144における処理としてホスト302側に転送される点が異なる。

【0147】

このようにして、ホスト302側から初期ベクトルIVの転送要求があると、ドライブ装置301は、初期ベクトルIVを生成し、ホスト302側に転送する。もちろん、ドライブ装置301は、生成した初期ベクトルIVを、ホスト302側に転送するだけでなく、自己の暗号化部312(図10)にも供給する。

【0148】

図12のフローチャートの処理の説明に戻り、ステップS39における初期ベクトルIVの転送の処理が終了されると、ステップS40(図13)に処理が進められる。ステップS40において、初期ベクトルIVの再発行要求があったか否かが判断される。ステップS40において、初期ベクトルIVの再発行要求があったと判断された場合、ステップS41乃至S43の処理が実行される。

【0149】

ステップS41乃至S43は、基本的に、ステップS37乃至ステップS38の処理と同様であるが、図16を参照して説明を加える。ホスト301は、ステップS161において、初期ベクトルIVの再発行要求をドライブ装置301に対して出す。この再発行要求は、コマンドパケット363が出力されることにより行われるが、このコマンドパケット363は、例えば、図14のステップS102において発行されるREPORT KEY commandと同じである。

【0150】

ドライブ装置301は、ステップS171において、REPORT KEY commandを受信すると、ステップS172において、初期ベクトルIVを再生成する。初期ベクトルIVの再生成は、図14のステップS113、または、図15のステップS143の処理と同様に行われる。そして、再生成された初期ベクトルIVは、ステップS173において、ホスト302側に転送される。この転送時に、初期ベクトルIVは、暗号化が施されて転送されるようにしても良いし、そのまま転送されるようにしても良い。

【0151】

図13のフローチャートの説明に戻り、ステップS40において、初期ベクトルIVの再発行要求がないと判断された場合、または、ステップS43における処理として初期ベ

クトルⅣの転送に関わる処理が終了した場合、ステップS44に処理が進められる。

【0148】

ステップS44において、セクタデータ351の転送要求があったか否かが判断される。この判断は、コマンド処理部317が、ホスト302側から、コマンドパケット363を受信したか否かを判断し、かつ、受信したコマンドパケット363が、セクタデータ351の転送を要求するものであるか否かを判断することにより行われる。

【0149】

ステップS44において、セクタデータ351の転送要求はないと判断された場合、ステップ40に処理が戻され、それ以降の処理が繰り返される。一方、ステップS44において、セクタデータ351の転送要求があったと判断された場合、ステップ45に処理が進められる。

【0150】

ステップS45において、セクタ転送カウンタ314のカウンタ値Nが、 $N > N_{max}$ という関係を満たすか否かが判断される。ステップS45において、 $N > N_{max}$ という関係は満たされていないと判断された場合、ステップS46に処理が進められる。 $N > N_{max}$ という関係が満たされていない状態、すなわち、 $N < N_{max}$ という関係を満たす状態のときには、セクタ転送制御部313からのデータの出力（ホスト302側へのデータの転送）が許可されている状態である。

【0151】

そこで、ステップS46においては、セクタ転送制御部313からホスト302側へのデータの転送が行われる。まず、コマンド処理部317の指示により、アクセス処理部318が、ディスク303からセクタデータ351の読み出しの制御を行う。アクセス処理部318の制御により、ディスク303から読み出されたセクタデータ351は、暗号化部312に供給される。

【0152】

暗号化部312は、認証処理部311から供給されるセッションキーKsと、乱数発生部315から供給される初期ベクトルⅣを用いて、セクタデータ351を暗号化する。暗号化されたセクタデータ351は、セクタ転送制御部313の制御により、ホスト302に転送される。この際、セクタデータ351が転送される経路は、UDF経路であり、そのデータ量は、2048バイト（または、2048の整数倍のバイト数）とされている。

【0153】

暗号化部312からデータが出力されると、その情報は、セクタ転送カウンタ314に供給される。セクタ転送カウンタ314は、ステップS47において、自己が管理しているカウンタ値Nを、 $N + 1$ の値に更新し、その更新された値を新たなカウンタ値Nと設定する。セクタ転送カウンタ314におけるカウンタ値Nの更新が終了されると、ステップS40に処理が戻され、それ以降の処理が繰り返される。

【0154】

このセクタデータ351の転送に関わる処理について、図17のタイミングチャートを参照して、説明を加える。ホスト302は、ステップS201において、リードコマンド(READ command)を発行する。リードコマンドは、ディスク303からセクタデータ351を指示する際に発行されるコマンドである。また、後述するように、ディスク303にデータを書き込む際にライトコマンド(WRITE command)が発行される。

【0155】

発行されるリードコマンドは、例えば、図18に示したデータ構成を有するコマンドパケット363の一種である。コマンドの詳細はINCITS T10 WORKING DRAFT “MultiMedia Command Set-4 (MMC-4)” に記述がある。

【0156】

図18に示したコマンドパケット363は、リードコマンドまたはライトコマンドの形式を示すものである。図18に示したコマンドパケット363内のデータのうち、以下の説明に必要な部分のデータについて説明を加える。

【0157】

“Operation Code”には、リードコマンドであるか、ライトコマンドであるかを示すデータが書き込まれる。よって、この部分に書き込まれているデータを参照することで、ホスト302からコマンドを受け取ったドライブ装置301は、リードコマンドであるか、ライトコマンドであるかを判別することが可能となっている。また、“Operation Code”は、1バイトのデータである。

【0158】

“Logical Block Address”には、コマンドパケット363がリードコマンドである場合には、読み出すべきアドレスの開始LBAが書き込まれ、コマンドパケット363がライトコマンドである場合には、書き込むべきアドレスの開始LBAが書き込まれている。また、“Logical Block Address”は、4バイトのデータである。

【0159】

“Transfer Length”には、コマンドパケット363がリードコマンドである場合には、読み出しセクタ数を指示するデータが書き込まれ、コマンドパケット363がライトコマンドである場合には、書き込みセクタ数を指示するデータが書き込まれる。また、“Transfer Length”は、4バイトのデータである。

【0160】

ステップS201において、ホスト302から発行されるコマンドパケット363は、“Operation Code”がリードコマンドを示す値が記載されているコマンドである。ここでは、その発行されるリードコマンドに含まれる“Transfer Length”は“N1”であるコマンドが発行されたとする。

【0161】

ステップS201における処理で発行されたリードコマンドは、ステップS231において、ドライブ装置301のコマンド処理部317に供給される。コマンド処理部317は、供給されたコマンドの“Operation Code”を参照し、リードコマンドであることを認識する。そして、“Logical Block Address”を参照し、データの読み出しを開始するアドレスを認識し、“Transfer Length”を参照して、この場合、“Transfer Length”=N3ということを認識する。

【0162】

コマンド処理部317は、認識結果を、アクセス処理部318に供給する。アクセス処理部318は、コマンド処理部317からの認識結果に基づき、ディスク303からのデータの読み出しを制御する。アクセス処理部318における処理としては、アドレスの変換処理などがある。

【0163】

アクセス処理部318は、LBA/PSN変換を行う。LBAは、Logical Block Addressの略であり、PSNは、Physical Sector Numberの略である。LBAは、論理的なアドレスを示し、例えば、リードコマンドに含まれ、ディスク303上の読み出すべきデータの物理媒体に依存せずにドライブ装置301とホスト302との間で共通的に扱うことを可能とする論理的なアドレスを示す。

【0164】

LBAに対し、PSNは、物理的なアドレスを示す。コマンドパケット363には、LBAが含まれるが、このLBAは、ディスク303上の論理的なアドレスを示し、実際の物理的なアドレスは示していないため、物理媒体から読み出した物理的なアドレスを示すPSNから共通に扱える論理的なアドレスへ変換するといった処理が、必要に応じ行われる。その変換処理を、アクセス処理部318は行う。

【0165】

なお、ディスク303上のユーザに開放された記録領域であるユーザデータエリア（不図示）の物理セクタに対して、例えば、ある物理セクタ番号の物理セクタを基準として、シーケンシャルな論理セクタ番号の論理セクタが、順次割り当てられる。変換方法の事例はINCITS T10 WORKING DRAFT “MultiMedia Command Set-4 (MMC-4)”に記述がある。

【0166】

LBAがPSNに変換されると、ステップS232の処理として、その変換されたPSNが指し示すディスク303上の位置が検索される。この検索の結果、ピックアップ(不図示)がディスク303上の、読み出すべき位置に移動されるなどの処理が実行され、ディスク303からセクタデータ351が読み出される。読み出されたセクタデータ351は、暗号化部312に供給される。

【0167】

暗号化部312には、認証処理部311からセッションキーKsが供給され、乱数発生部315から初期ベクトルIVも供給される。暗号化部312は、供給されたセッションキーKsと初期ベクトルIVを用いてセクタデータ351を暗号化する。暗号化されたセクタデータ351(この場合、Encrypted Sector Data #1)は、ステップS232の処理として、セクタ転送制御部313の制御のもと、ホスト302の復号部322に対して出力される。

【0168】

復号部322は、供給されたEncrypted Sector Data #1を、認証処理部321から供給されるセッションキーKsと、ドライブ装置301の乱数発生部315から供給された初期ベクトルIVを用いて復号し、セクタデータ361を生成する。このようにして生成されたセクタデータ361は、図示されていないアプリケーションソフトウェアやディスプレイヤスピーカに提供される。

【0169】

このような処理がドライブ装置301とホスト302間で繰り返される。ドライブ装置301から、順次、Physical Sector Dataが読み出される。すなわち、ディスク303側からは、ドライブ装置301の検索制御に応じて順次、連続的にセクタデータが読み出されドライブ装置301に供給される。

【0170】

ドライブ装置301は、ステップS233乃至S240の各ステップの処理において、順次、読み出したセクタデータを暗号化し、ホスト302の要求(リードコマンドの発行)に応じてホスト302に供給する。

【0171】

ドライブ装置301は、ホスト302に対してセクタデータを転送する際、セクタ転送カウンタ314により管理されているカウンタ値Nの更新処理なども行う。例えば、ステップS232の処理として、セクタデータ351が暗号化されてホスト302側に転送されると、セクタ転送カウンタ314のカウンタ値Nは、1だけ増加された値に更新される(ステップ47の処理)。よって、このようなカウンタ値Nの更新の処理が繰り返される(セクタデータが、順次、ホスト302側に転送されると)、カウンタ値Nの値が、閾値Nmaxよりも大きくなる(N>Nmaxを満たす)ときがある。

【0172】

図17を参照するに、(N1+N2) < Nmax < (N1+N2+N3)と設定されているとする。このような場合、ステップS240において、(N1+N2+1)番目のセクタデータが転送された後の時点(セクタ転送カウンタ314が管理するカウンタ値Nが、(N1+N2+1)となった後の時点)で、順次、セクタデータがディスク303から読み出され、暗号化され、転送されという処理が繰り返されると、カウンタ値Nの値は、順次1つずつ増加されるので、N>Nmaxという条件を満たすようになる。

【0173】

N>Nmaxという条件が満たされると、すなわち、ステップS45(図13)において、YESと判断されると、ステップS48(図17においては、ステップS241)に処理が進められる。

【0174】

ステップS48(ステップS241)において、エラーメッセージ(Error Message)がドライブ装置301からホスト302側に出力される。ドライブ装置301のセクタ転送

カウンタ314は、自己がカウントしているカウンタ値Nが、閾値N_{max}よりも大きくなつたと判断したとき、セクタ転送制御部313に対して、暗号化部312から供給されるデータをホスト301側に出力しないように指示を出す。

【0175】

セクタ転送制御部313は、セクタ転送カウンタ314から、出力停止の指示を受けると、セクタデータの出力を停止すると共に、メッセージ伝達部316に対して、出力停止の指示を受けたことを知らせる。メッセージ伝達部316は、セクタ転送制御部313から、出力停止の指示を受けたという知らせを受けると、エラーメッセージを作成し、ホスト302に対して送信する。このエラーメッセージは、ホスト302に、指示されたデータの供給はできないということを認識させるためのメッセージである。

【0176】

このようなメッセージが出力されると、ドライブ装置301側からはデータが出力されない状態とされる。換言すれば、ドライブ装置301側で、認証処理が正常に行われた結果、データの出力が許可された状態であっても、その状態が解除され、許可されない状態に変更される。

【0177】

このように、本実施の形態によれば、一度設定されたデータ出力の許可という状況を変更することが可能である。よって、エラーメッセージが出力された後、ホスト302から、ディスク303からのデータの読み出しが指示されても、その指示に対応して、データが読み出されることはない。

【0178】

エラーメッセージが出力されると、ドライブ装置301からホスト302へのデータの出力が停止される。このようなデータの出力が停止されてしまふ状況が発生しないようにするためには、ホスト302側で、初期ベクトルIVの発行要求が、所定のタイミングでドライブ装置301に対して出されればよい。

【0179】

すなわち、初期ベクトルIVの発行が要求されれば（例えば、ステップS40（図13））、セクタ転送カウンタ314のカウンタ値Nが0にリセットされる（ステップS42）。その結果、N>N_{max}という条件が満たされることを回避できるため、エラーメッセージが出力されるような状況が発生する（ステップS48）ようなことを回避することができる。

【0180】

ホスト302は、定期的に初期ベクトルIVの発行の要求を出す。定期的とは、例えば、初期ベクトルIVの発行を要求した後、転送を指示したデータ量の累計が所定のデータ量（例えば、16Mbyte (8K Sector)）を超える毎に要求されるということである。または、初期ベクトルIVの発行を要求した後、所定の時間が経過する毎に要求されるということである。

【0181】

いずれにしても、ホスト302は、所定のタイミングで、初期ベクトルIVの発行の要求を出す。よって、正常に（正当に）処理が実行されている間、ドライブ装置301側では、ステップS41乃至S43の処理が定期的に行われることになり、定期的にセクタ転送カウンタ314のカウンタ値Nが0に設定されることになる。

【0182】

このようにすることで、少なくとも以下のような問題を解決することができる。

ドライブ装置301とホスト302との間で一旦、相互認証が成功したら、ドライブ装置301は、相手（ホスト302において起動されているアプリケーションなど）が正当であろうが、正当でなかろうが、保護されたデータを相手側の指示に従って出力してしまうといった問題。

バスを第3者が観測し、保護されたデータを横取りして解読し平文化してしまうといった問題（不正に利用されてしまうという問題）。

【0183】

このような問題を解決するために、上述したように、まず、保護されたデータ（ディスク303に記録されているセクタデータ351）をドライブ装置301からホスト302にバス転送する際、その保護されたデータをセッションキーKsで暗号化してから転送するようにした。このことにより、仮に、バスを第3者が観測し、保護されたデータを横取りしたとしても、そのデータを解読し平文化することを困難にすることが可能となる。

【0184】

そして、データを暗号化する際、初期ベクトルIVを適用するようにした。またその初期ベクトルIVは、乱数を用いてランダムに変更されるようにした。このようにすることで、仮に、第3者が何らかの方法で、保護されたデータを横取りしたとしても、そのデータを解読し平文化することをより困難にすることが可能となる。

【0185】

また、初期ベクトルIVが変更されるようすることで、平文データが特別なデータであることを特定させることを困難にすることが可能となる。このことは、データのすり替えや、データの改竄など、不正な行為を防止できることを意味する。さらに、初期ベクトルIVを適宜更新することで、大量のデータを单一の鍵で暗号化した場合に、暗号鍵（セッションキーKs）が予測されやすくなるといった問題を解決することが可能となる。

【0186】

また、上述したように、本実施の形態によれば、ホスト302側から適切に初期ベクトルIVの更新が指示されなければ、データの供給が停止されるため、ドライブ装置301とホスト302との間で一旦、相互認証が成功したら、ドライブ装置301は、相手（ホスト302において起動されているアプリケーションなど）が正当であろうが、正当でなかろうが、保護されたデータを相手側の指示に従って出力してしまうといった問題を解決することができる。

【0187】

すなわち、正当なドライブ装置301は、正当なホスト302にのみ、保護されたデータを転送するように制御することが可能となる。

【0188】

上述した実施の形態においては、初期ベクトルIVが更新されたが、暗号化に用いられるセッションキーKs自体が更新されるようにしても良い。換言すれば、ホスト302からは、初期ベクトルIVの再発行の指示が出されるのではなく、セッションキーKsの再発行の処理が出されるようにしても良い。

【0189】

しかしながら、セッションキーKsは、相互認証が正常に終了されなければ生成されないため、セッションキーKsの更新に係る処理時間や処理能力を考慮すると、初期ベクトルIVの方を更新する方が好ましいと考えられる。

【0190】

上述した実施の形態においては、ディスク303からデータを読み出す（再生）の場合を例に挙げて説明したが、本発明はデータの再生にのみ適用範囲が限定されるわけではない。すなわち、本発明を、ディスク303へのデータの書き込み（記録）に適用することも可能である。

【0191】

図19は、本発明を記録装置に適用した場合のシステム構成例を示す図である。

【0192】

図19に示し記録装置のドライブ装置401は、ホスト402から供給されるデータを、セットされているディスク303に記録する。ドライブ装置401は、認証処理部411、復号部412、セクタ転送制御部413、セクタ転送カウンタ414、乱数発生部415、メッセージ伝達部416、コマンド処理部417、および、アクセス処理部418を含む構成とされている。

【0193】

ホスト402は、認証処理部421、暗号化部422を含む構成とされている。

【0194】

図19に示した記録装置の構成は、図10に示した再生装置の構成と同様な部分が多いので、その詳細な説明は省略し、異なる部分についてのみ説明を加える。

【0195】

図19に示した記録装置は、ディスク403にセクタデータを451を記録する。この記録されるセクタデータ451は、ホスト402側から供給されるセクタデータ461である。ホスト402の暗号化部422は、図示されていない記録媒体またはハードディスクドライブなどから読み出されたセクタデータ461を、認証処理部421から供給されるセッションキーKsを用いて暗号化する。

【0196】

暗号化部422により暗号化されたセクタデータ461は、ドライブ装置401のセクタ転送制御部413に供給される。セクタ転送制御部413は、供給されたセクタデータ461を、復号部412に供給する。復号部412は、供給されたセクタデータ461を、認証処理部411から供給されるセッションキーKsを用いて復号する。復号されたセクタデータ461は、セクタデータ451として、アクセス処理部418の制御のもと、ディスク403に記録される。

【0197】

セクタ転送カウンタ414は、セクタ転送制御部413から出力され、復号部412に供給されたセクタ数をカウントする。その他の部分に関しては、図10に示した再生装置の対応する部分と、基本的に同様な構成であり、その動作も同様である。

【0198】

図19に示した記録装置のドライブ装置401は、既に図12、図13のフローチャートを参照して説明した処理と、基本的に同様な処理を実行するため、詳細な説明は省略する。ここでは、再度、図12、図13のフローチャートを参照し、異なる処理のみに説明を加える。

【0199】

ドライブ装置401は、ステップS44において、セクタデータの記録の要求があったか否かを判断する。この判断は、コマンド処理部417が、ホスト402側から、コマンドパケット463を受信したか否かを判断し、かつ、受信したコマンドパケット463が、セクタデータ461の書き込みを要求するもの（すなわち、ライトコマンド）であるか否かを判断することにより行われる。

【0200】

また、ステップS46においては、暗号化されたセクタデータ461が供給されるため、復号部412における復号処理が行われ、その復号されたセクタデータ461（451）がディスク403に書き込まれる処理が実行される。その他の処理については、基本的に同様であり、ホスト402から定期的に初期ベクトルIVの発行要求が出されなければ、ドライブ装置401側における書き込みの処理が停止される（ホスト403からのデータの出力が停止される）ように制御される。

【0201】

よって、ホスト402側で管理している保護されたデータが、不正に出力されること、そして、ディスク403に書き込まれてしまふことを防ぐことが可能となる。

【0202】

図20のタイミングチャートを参照して、図19に示した記録装置における、データの記録に関する処理について説明を加えるが、基本的な処理は、図17に示したタイミングチャートと同様であるので、その詳細な説明は省略する。異なる処理としては、ステップS301において、ホスト402から、データの書き込みを指示するライトコマンド(WRITE command)が送信される。

【0203】

また、ステップS302において、ホスト402の暗号化部422は、セクタデータ4

61をセッションキーKsを用いて暗号化し、その暗号化したデータ（Encrypted Sector Data #1）を、ドライブ装置401に対して送信する。ドライブ装置401のセクタ転送制御部423は、供給されたEncrypted Sector Data #1を、復号部412に供給する。

【0204】

復号部412は、認証処理部411から供給されるセッションキーKsと、乱数発生部415から供給された初期ペクトルIVを用いて復号し、セクタデータ451を生成する。このようにして生成されたセクタデータ451は、アクセス処理部418の制御に基づき、ディスク403に書き込まれる。

【0205】

このような処理が行われると共に、セクタ転送カウンタ414は、セクタ転送制御部413から出力されたセクタ数をカウントする。そして、そのカウントされているカウンタ値Nが、Nmax以上になったか否かの判断を行う。カウンタ値Nが大きくなると、すなわち、セクタデータが、順次、セクタ転送制御部413から出力されると、カウンタ値Nの値が、閾値Nmaxよりも大きくなる（N>Nmaxを満たす）ときがある。

【0206】

図20を参照するに、 $(N_1 + N_2) < N_{max} < (N_1 + N_2 + N_3)$ と設定されているとする。このような場合、ステップS340において、 $(N_1 + N_2 + 1)$ 番目のセクタデータが受信された後の時点（セクタ転送カウンタ414が管理するカウンタ値Nが、 $(N_1 + N_2 + 1)$ となった後の時点）で、継続的に、セクタデータがディスク403に書き込まれるという処理が繰り返されると、カウンタ値Nの値は、順次1つづ増加されるので、N>Nmaxという条件を満たすようになる。

【0207】

$N > N_{max}$ という条件が満たされると、すなわち、ステップS45（図13）において、YESと判断されると、ステップS48（図20においては、ステップS341）に処理が進められる。

【0208】

ステップ48（ステップS341）において、エラーメッセージ（Error Message）がドライブ装置401からホスト402側に出力される。ドライブ装置401のセクタ転送カウンタ414は、自分がカウントしているカウンタ値Nが、閾値Nmaxよりも大きくなつたと判断したとき、セクタ転送制御部413に対して、復号部412にデータを出力しないように指示を出す。

【0209】

セクタ転送制御部413は、セクタ転送カウンタ414から、出力停止の指示を受けると、セクタデータの出力を停止すると共に、メッセージ伝達部416に対して、出力停止の指示を受けたことを知らせる。メッセージ伝達部416は、セクタ転送制御部413から、出力停止の指示を受けたという知らせを受けると、エラーメッセージを作成し、ホスト402に対して送信する。このエラーメッセージは、ホスト402に、指示されたデータの書き込みはできないということを認識させるためのメッセージである。

【0210】

このようなメッセージが出力されると、ドライブ装置401側からはデータが入力されない状態とされる。また、エラーメッセージを受け取ったホスト402は、データを出力しない状態とされる。

【0211】

このように処理が行われることで、既に説明した再生装置の場合と同様の効果を望むことが可能である。

【0212】

このように、本発明を適用することにより、ドライブ装置とホストとの間で行われるデータの授受に関し、セキュリティを向上させることが可能となる。

【0213】

なお、上述した実施の形態においては、再生装置（図10）と記録装置（図19）をそ

それぞれ別な構成として図示および説明したが、再生装置と記録装置を同一の装置内に納めることも可能である。同一の装置内に納めるようにした場合、再生装置内と記録装置内において同一の処理を実行する、例えば、乱数発生部315(415)などは、再生装置と記録装置で共用される構成としても、もちろん良い。

【0214】

なお、上述した実施の形態においては、暗号化および復号の方式として、CBC方式を例に挙げて説明したが、本発明は、CBC方式にのみ適用できることを示すものではない。例えば、CFB(Cipher Feed Back)方式、OFB(Output Feed Block)方式などに對しても本発明を適用することはできる。

【0215】

上述した一連の処理は、それぞれの機能を有するハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、記録各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【0216】

記録媒体は、その記録媒体を扱うパーソナルコンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク(フレキシブルディスクを含む)、光ディスク(CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む)、光磁気ディスク(MD(Mini-Disc)(登録商標)を含む)、若しくは半導体メモリなどよりなるパッケージメディアにより構成されるだけである。コンピュータに予め組み込まれた状態でユーザに提供される、プログラムが記憶されているROMやハードディスクなどで構成される。

【0217】

なお、本明細書において、媒体により提供されるプログラムを記述するステップは、記載された順序に従って、時系列的に行われる処理は勿論、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0218】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【図面の簡単な説明】

【0219】

【図1】従来の再生装置の一例の構成を示す図である。

【図2】従来の再生装置の他の構成例を示す図である。

【図3】認証処理について説明するためのフローチャートである。

【図4】暗号化を行う回路の構成例を示す図である。

【図5】復号を行う回路の構成例を示す図である。

【図6】従来の再生装置における問題点を説明するための図である。

【図7】従来の再生装置における問題点を説明するための図である。

【図8】初期ベクトルIVを授受する際の問題点を説明するための図である。

【図9】初期ベクトルIVを授受する際の問題点を説明するための図である。

【図10】本発明を適用したシステムの一実施の形態の構成を示す図である。

【図11】データの授受に係わるドライバーについて説明するための図である。

【図12】ドライブ装置の動作について説明するためのフローチャートである。

【図13】図12のフローチャートに続くフローチャートである。

【図14】初期ベクトルIVの授受に関するタイミングチャートである。

【図15】初期ベクトルIVの授受に関するタイミングチャートである。

【図16】初期ベクトルIVの授受に関するタイミングチャートである。

【図17】データの授受に関するタイミングチャートである。

【図18】コマンドパケットの構成を示す図である。

【図19】本発明を適用したシステムの他の実施の形態の構成を示す図である。

【図20】データの授受に関するタイミングチャートである。

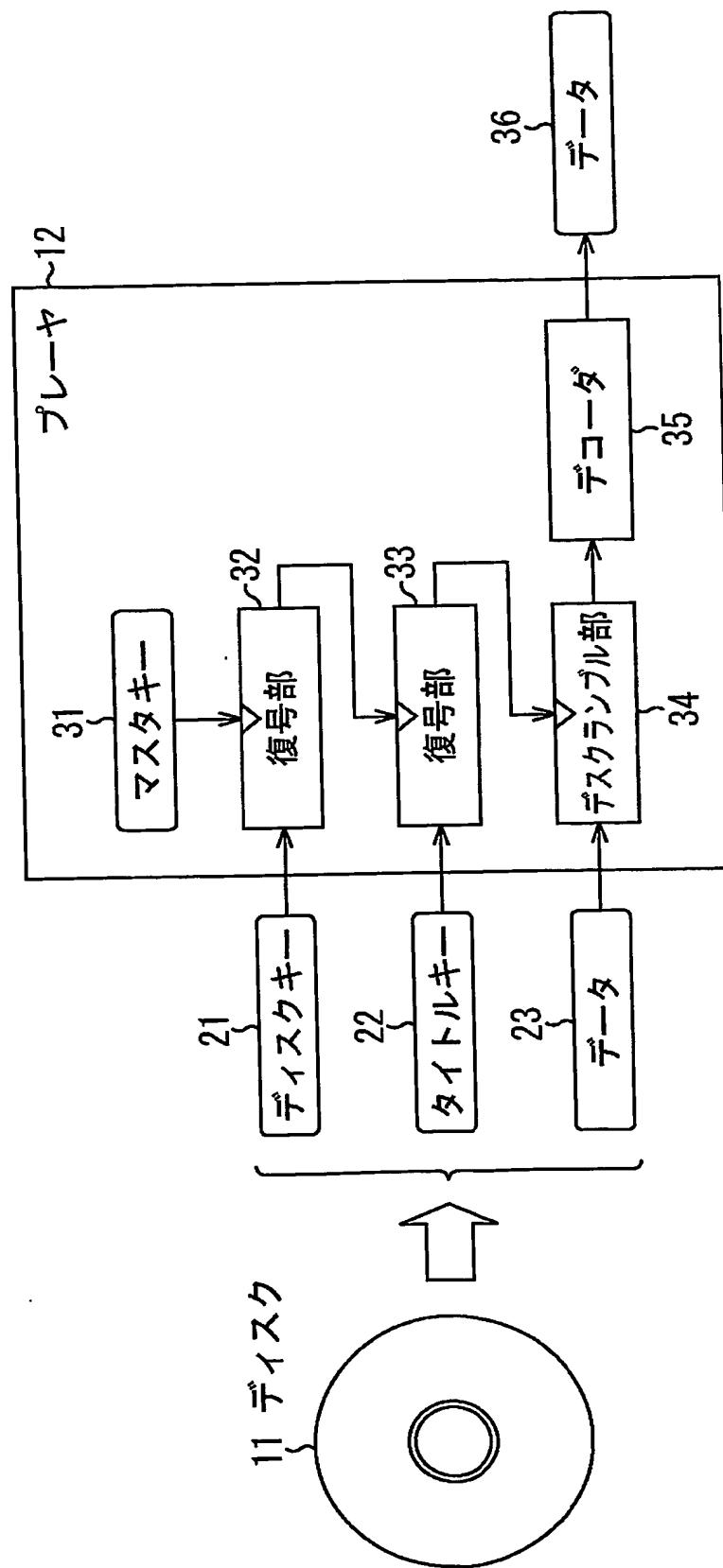
【符号の説明】

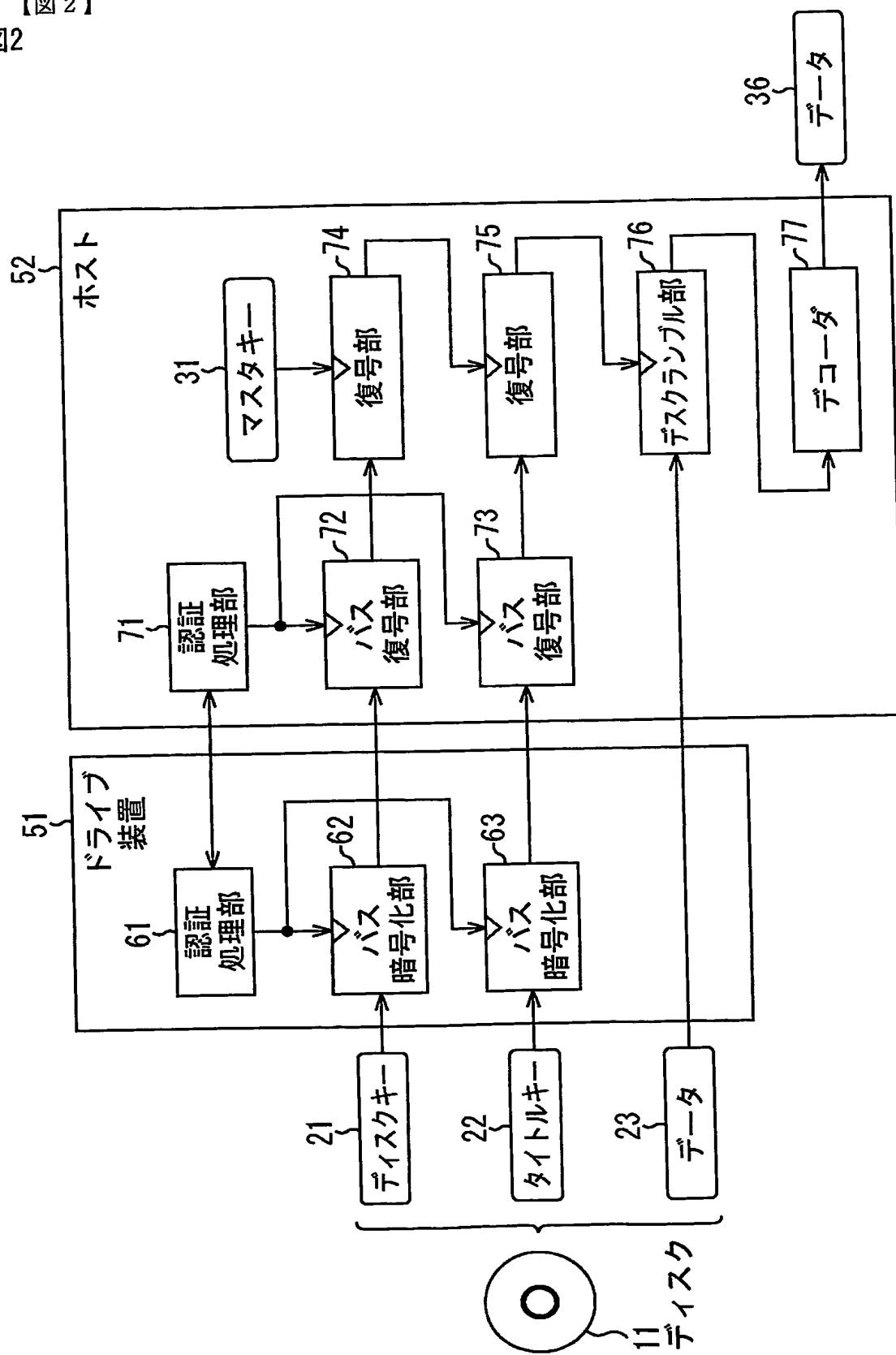
【0220】

301 ドライブ装置, 302 ホスト, 303 ディスク, 311 認証処理部, 312 暗号化部, 313 セクタ転送制御部, 314 セクタ転送カウンタ, 315 乱数発生部, 316 メッセージ伝達部, 317 コマンド処理部, 318 アクセス処理部, 321 認証処理部, 322 復号部, 401 ドライブ装置, 402 ホスト, 403 ディスク, 411 認証処理部, 412 復号部, 413 セクタ転送制御部, 414 セクタ転送カウンタ, 415 乱数発生部, 416 メッセージ伝達部, 417 コマンド処理部, 418 アクセス処理部, 421 認証処理部, 422 暗号化部

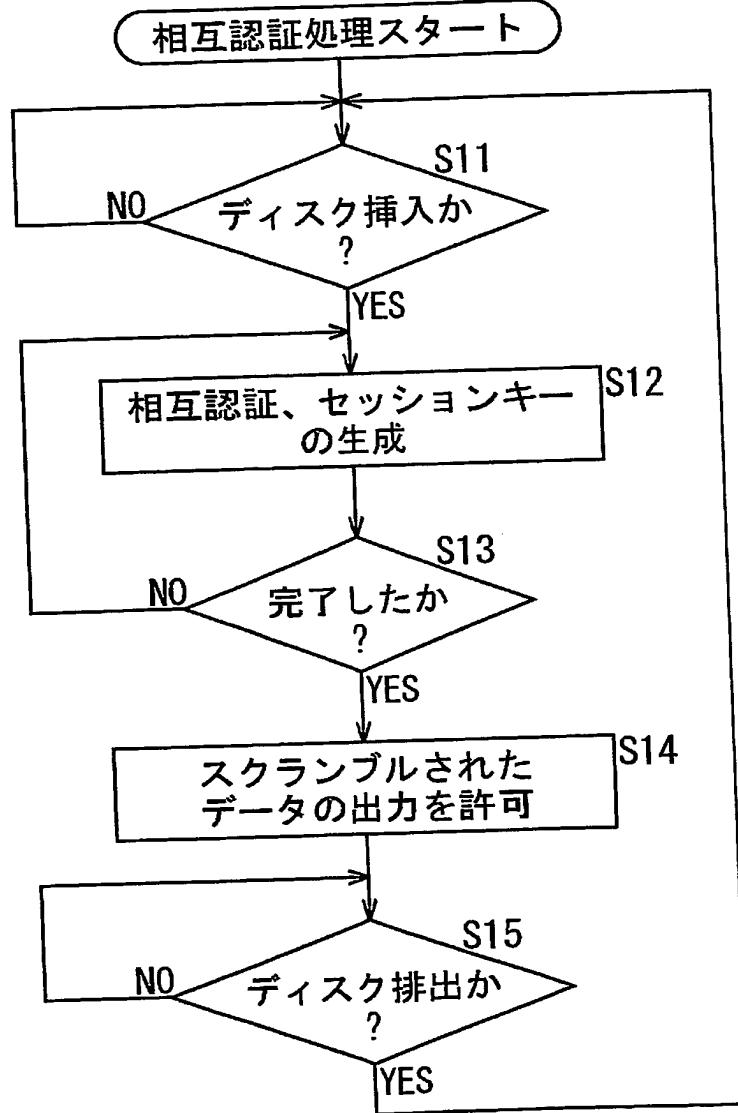
【書類名】 図面
【図 1】

図1



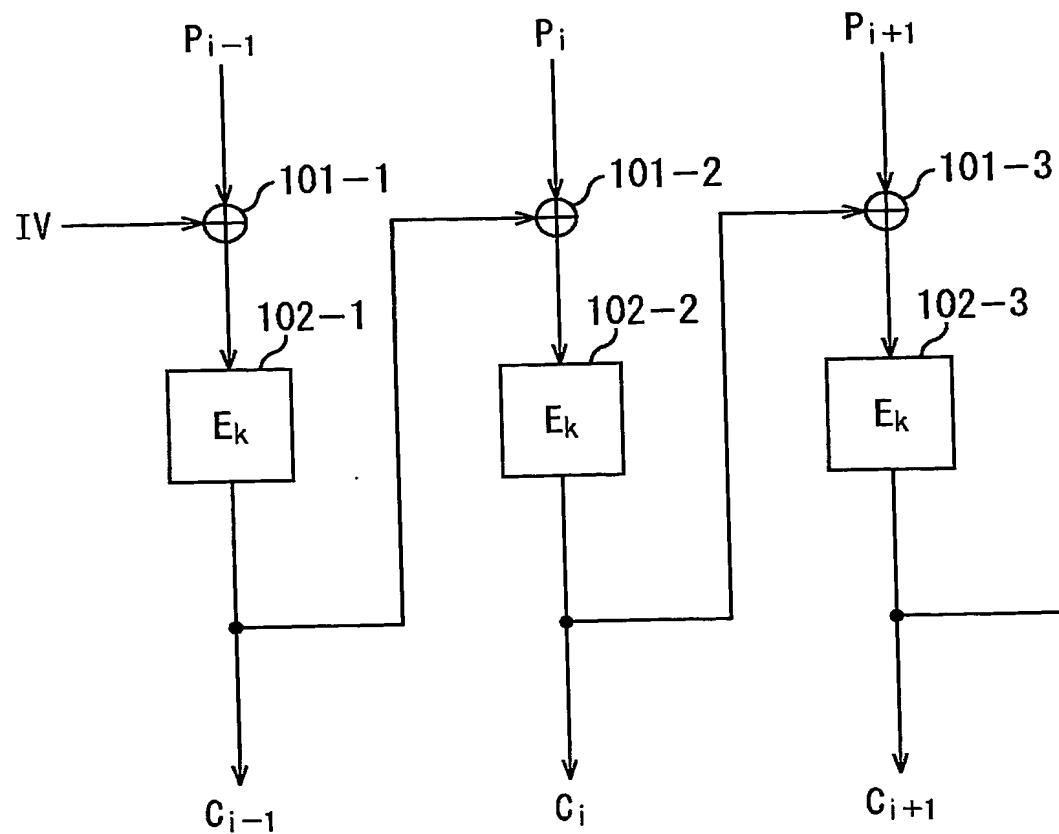
【図2】
図2

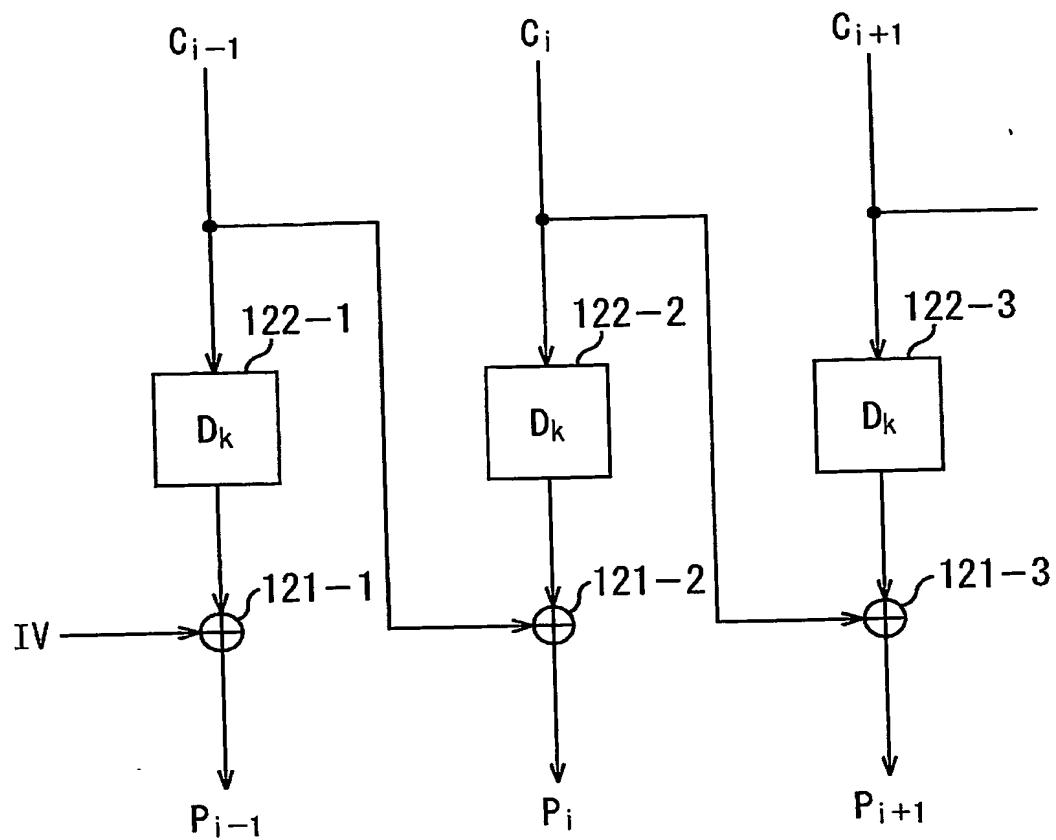
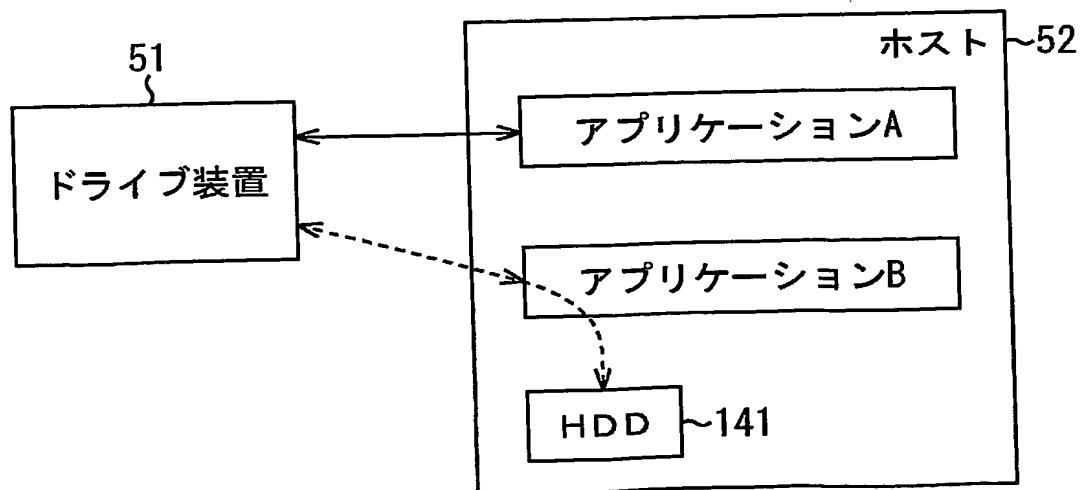
【図3】
図3

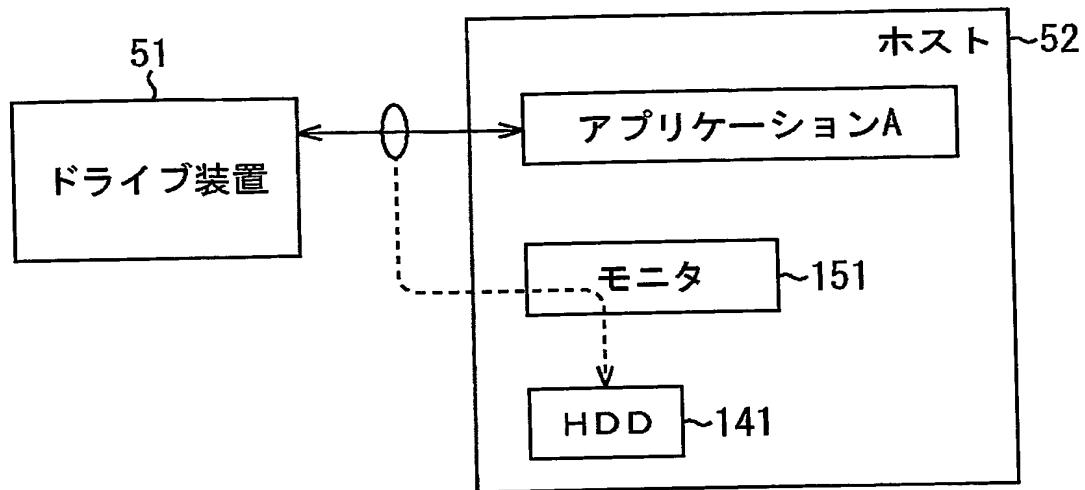


【図4】

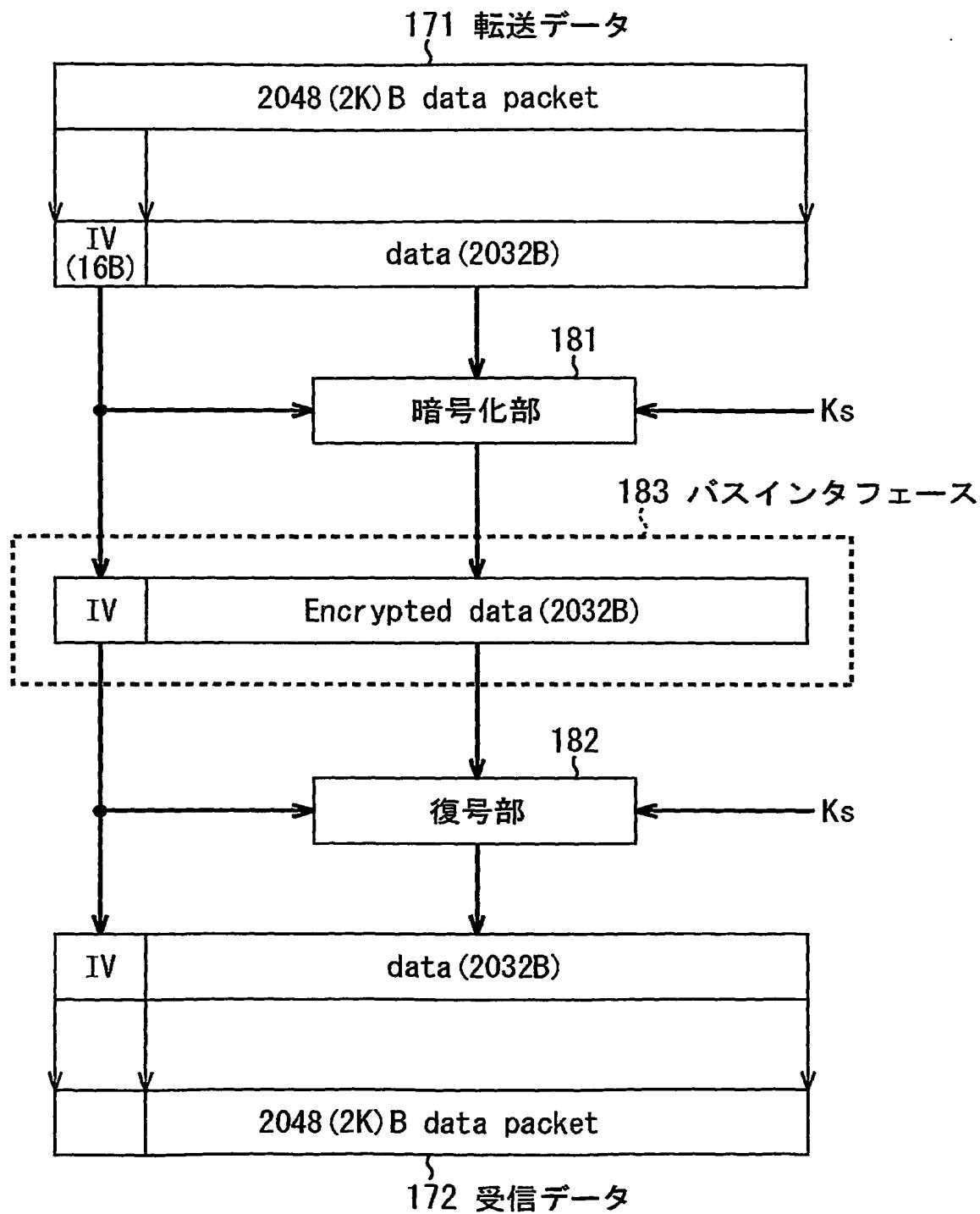
図4



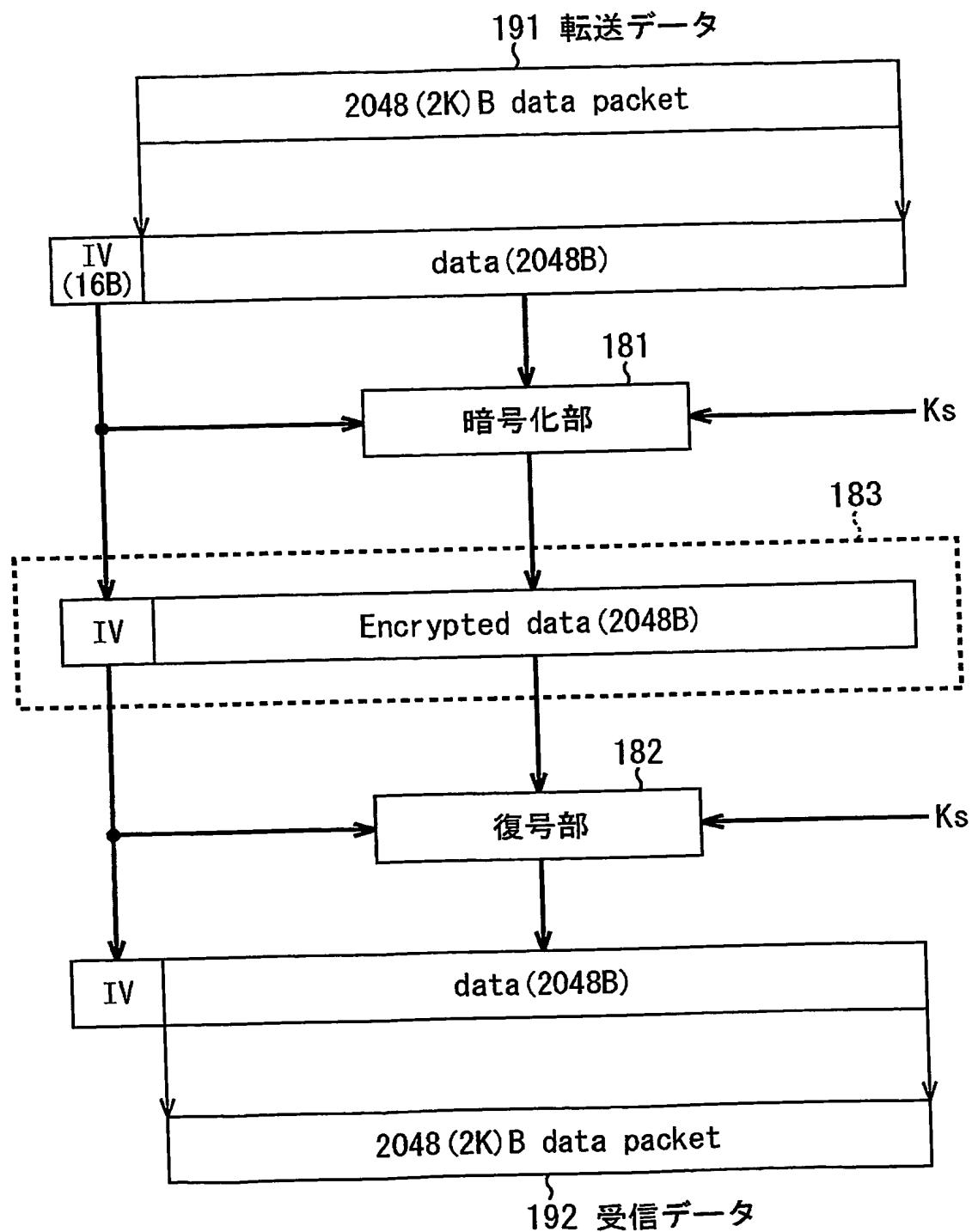
【図5】
図5【図6】
図6

【図7】
図7

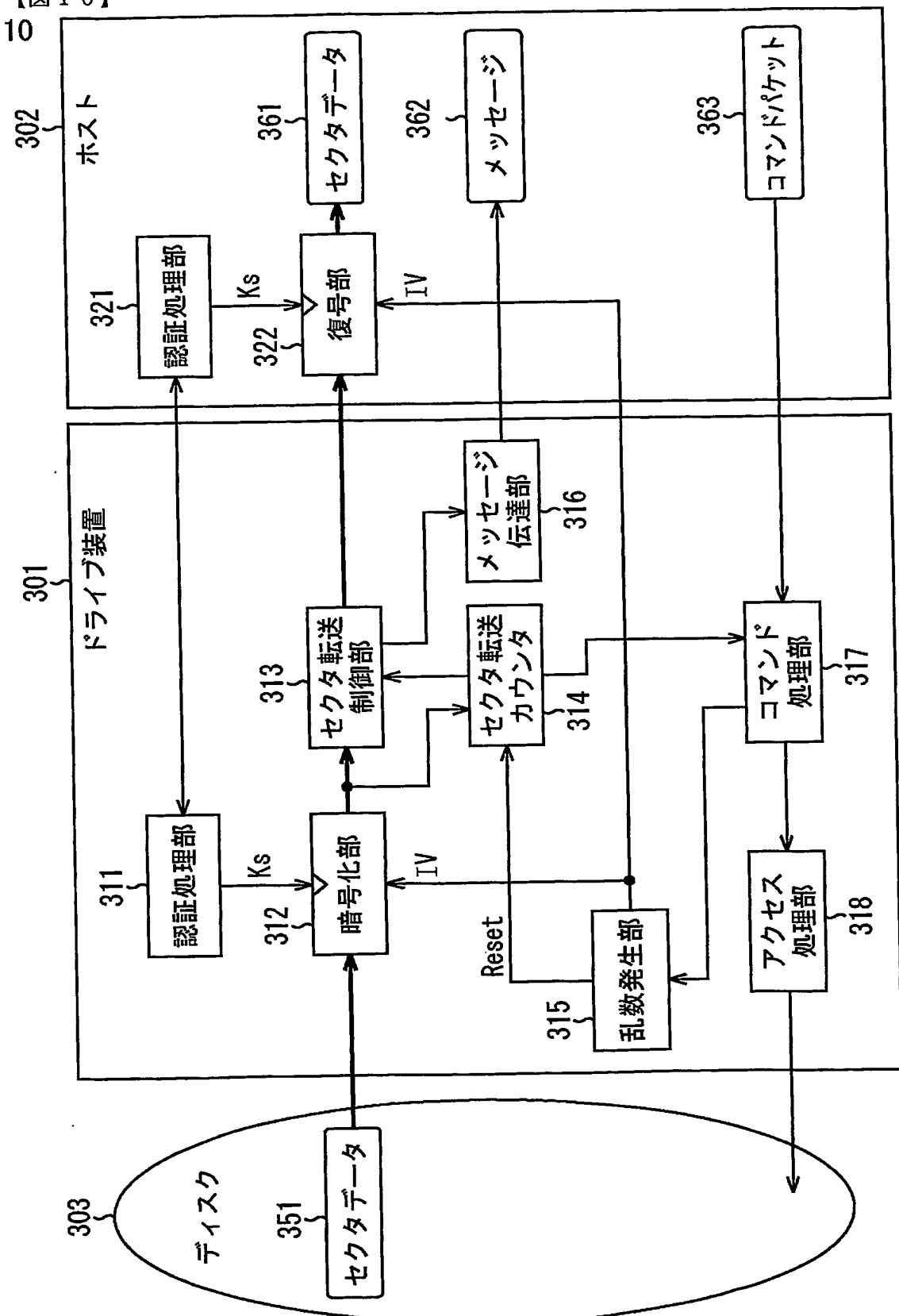
【図8】
図8

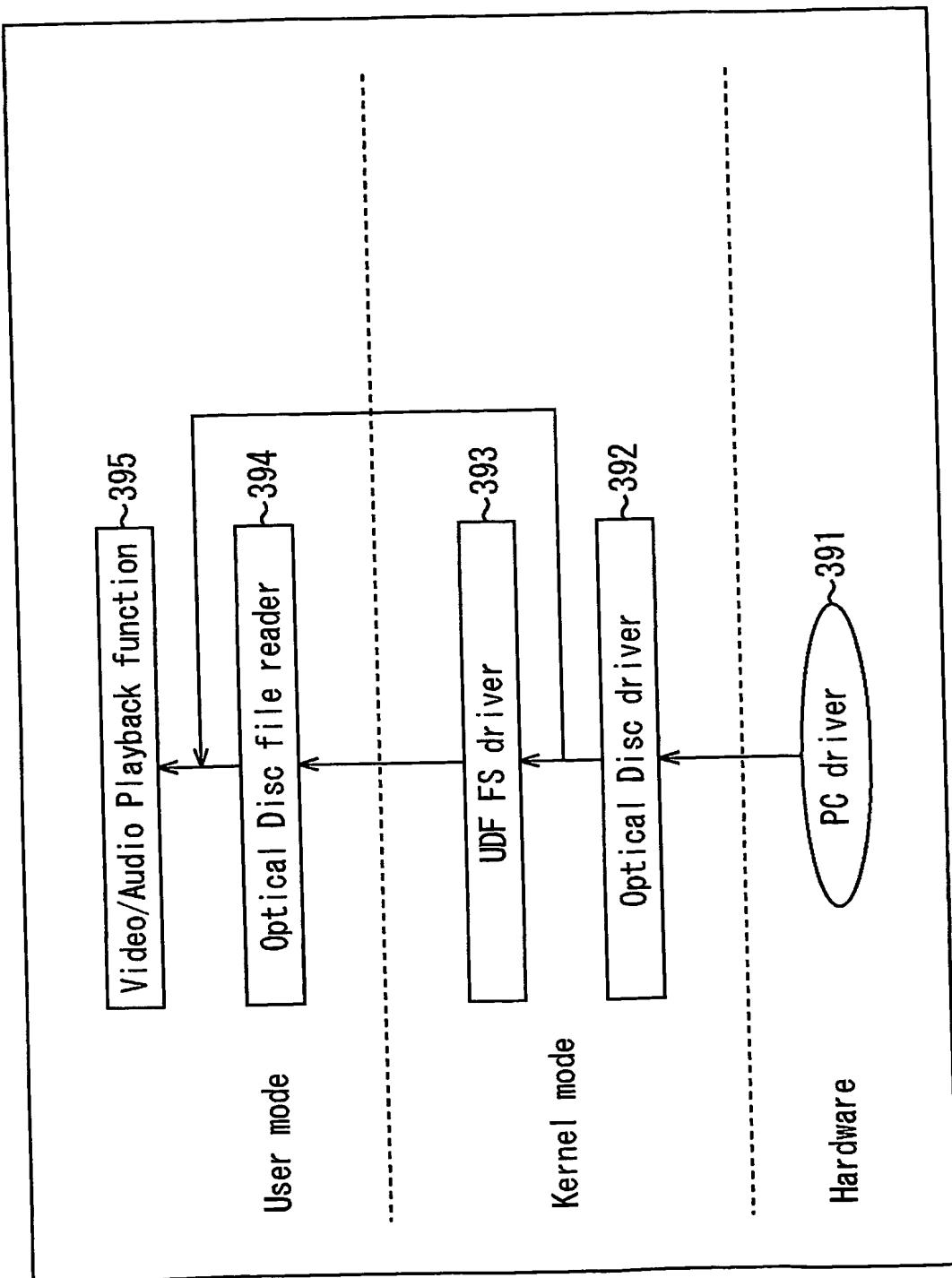


【図9】
図9

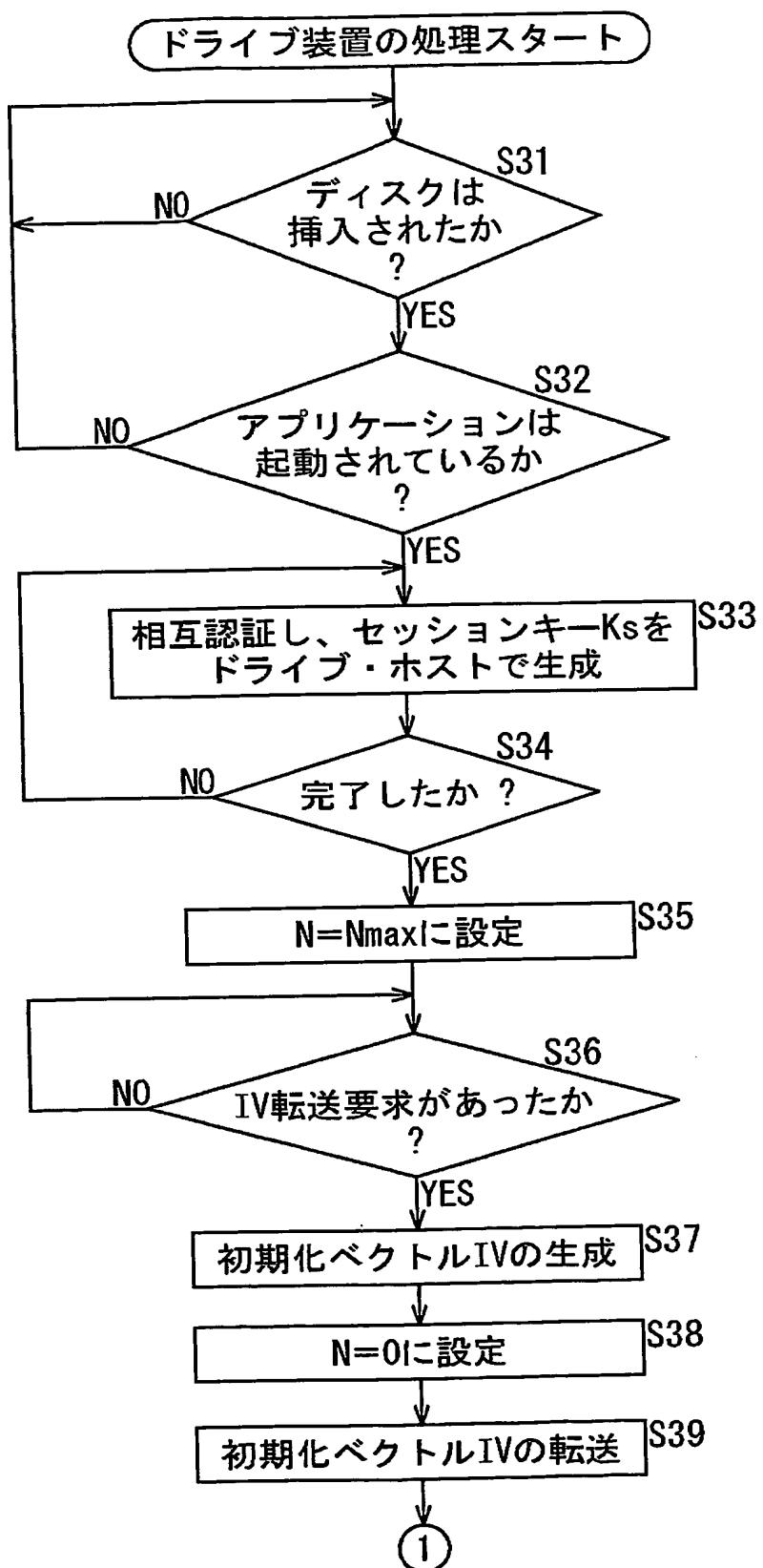


【図10】

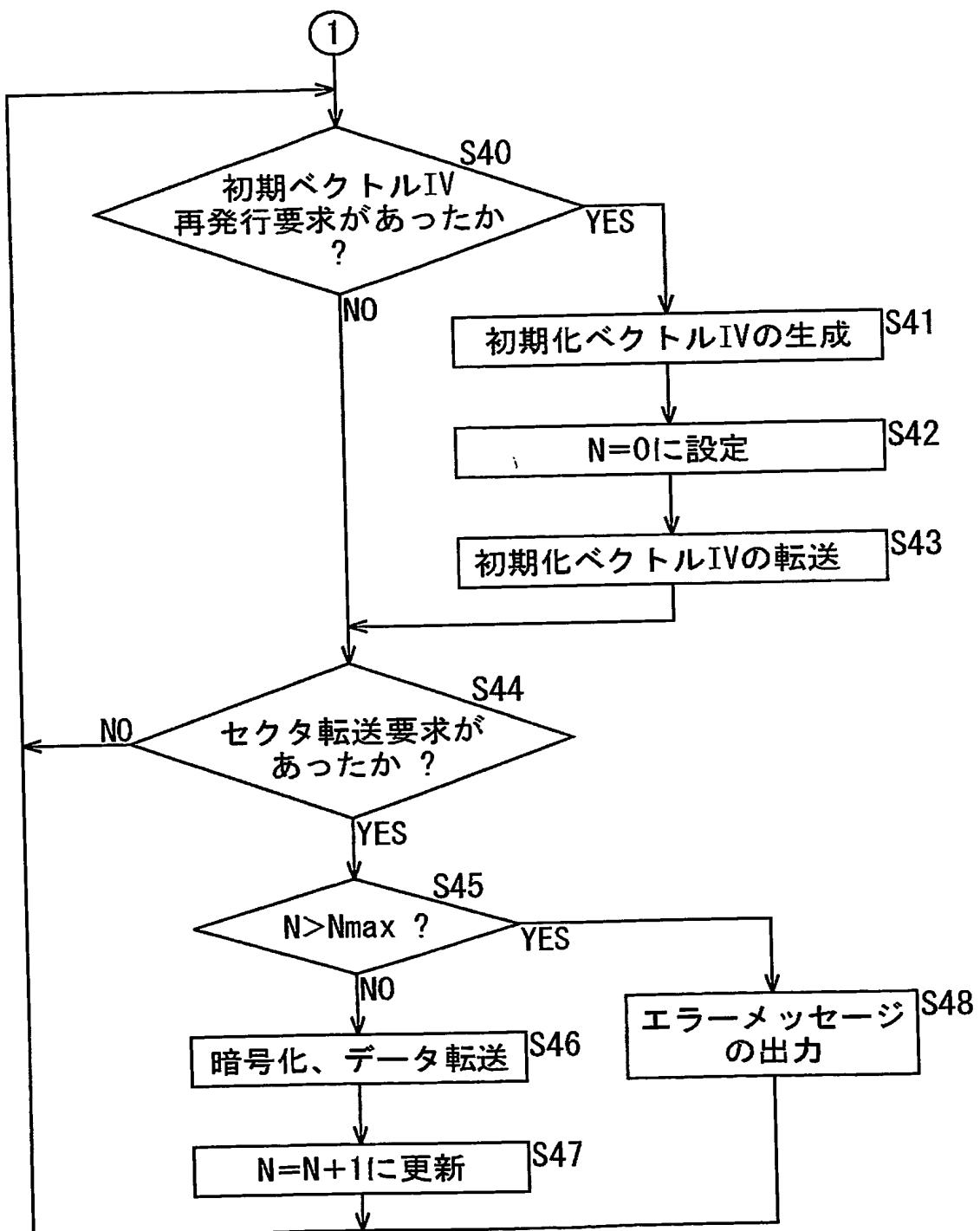


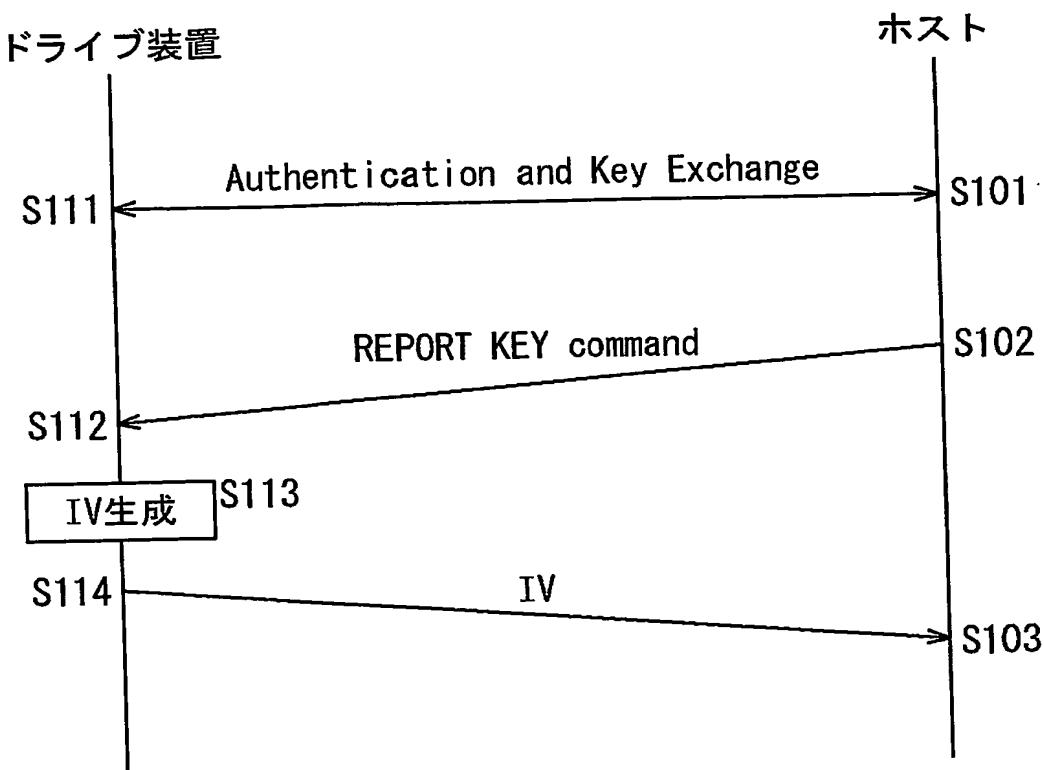
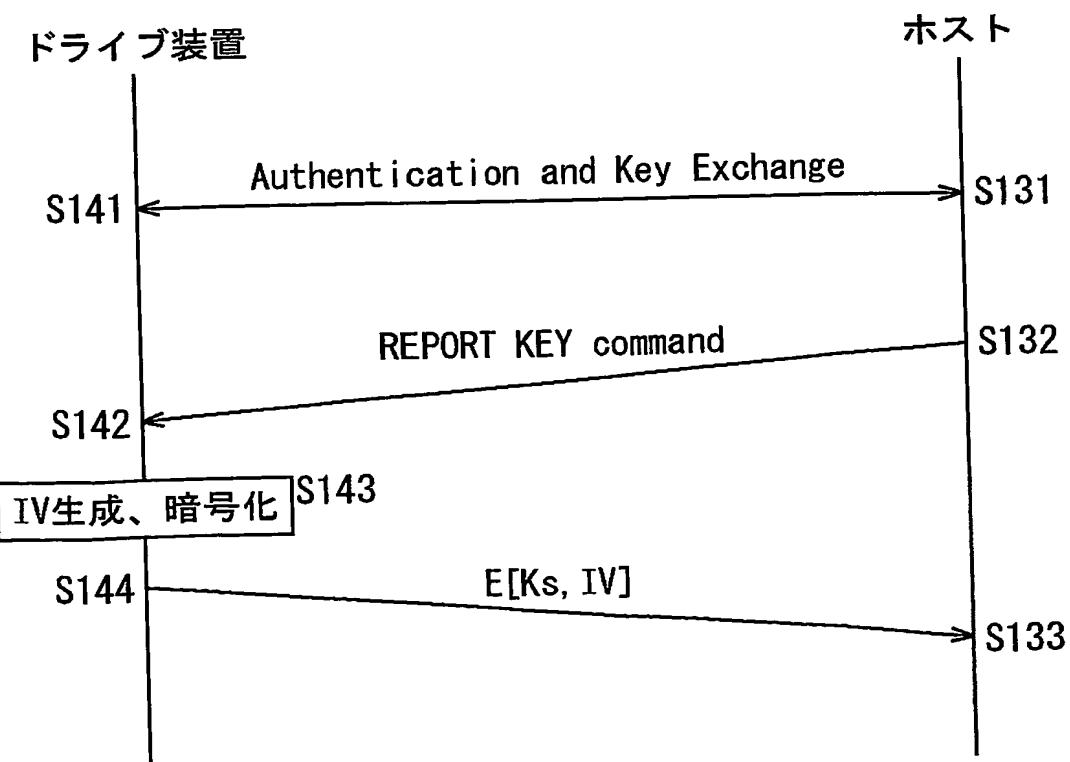
【図11】
図11

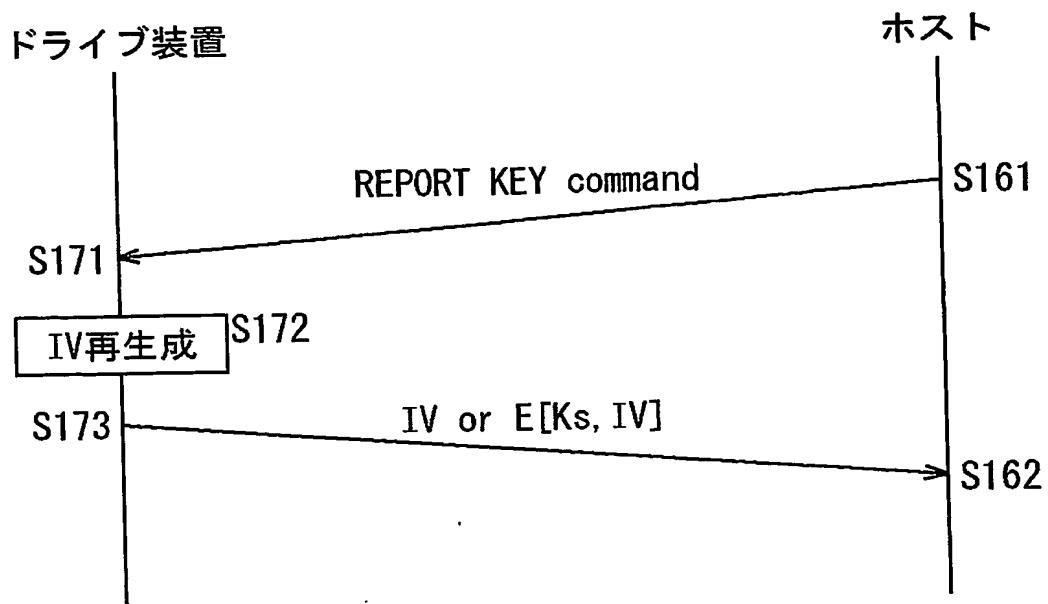
【図12】
図12
(12-1)



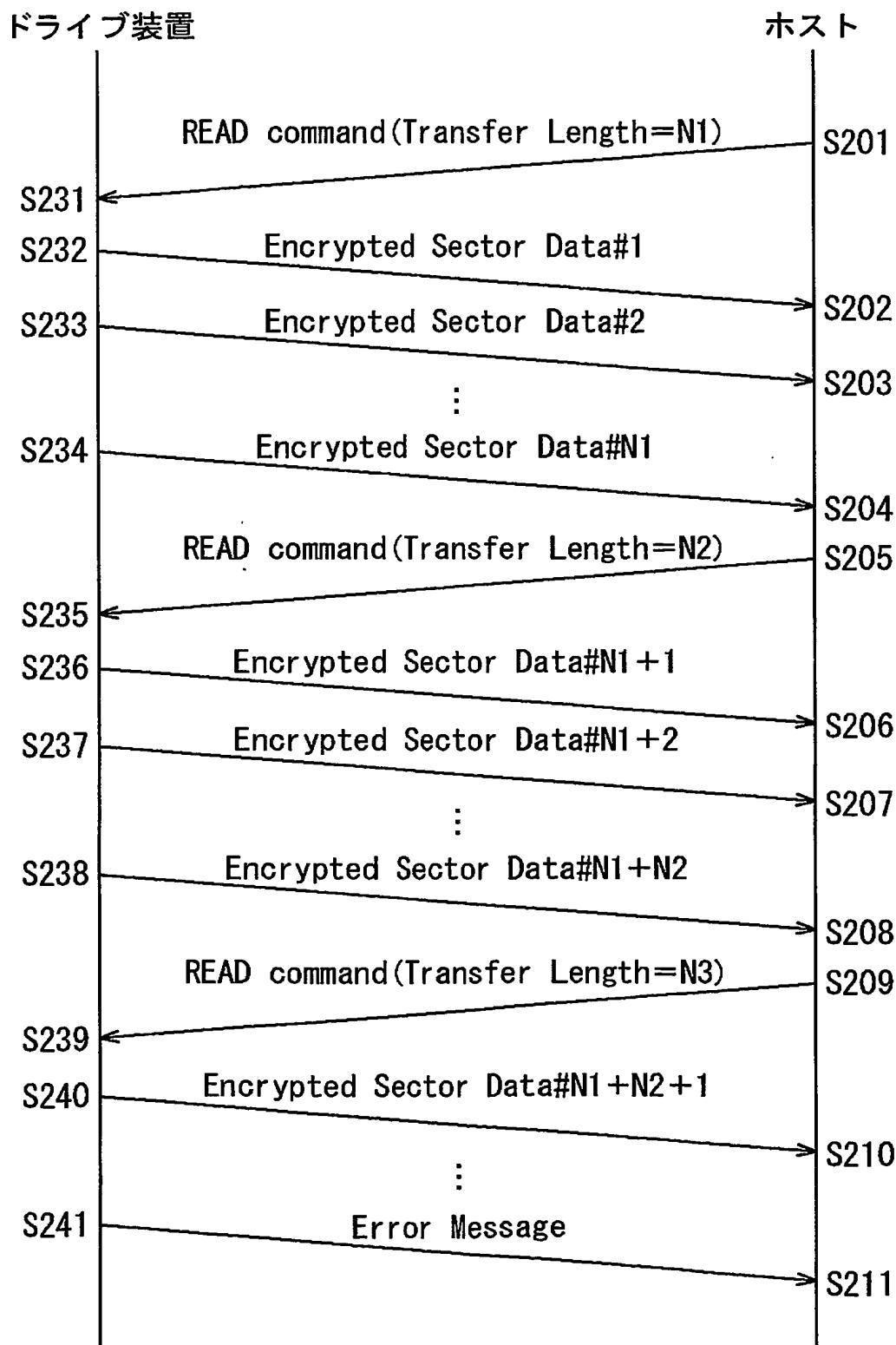
【図13】
図13
(12-2)



【図14】
図14【図15】
図15

【図16】
図16

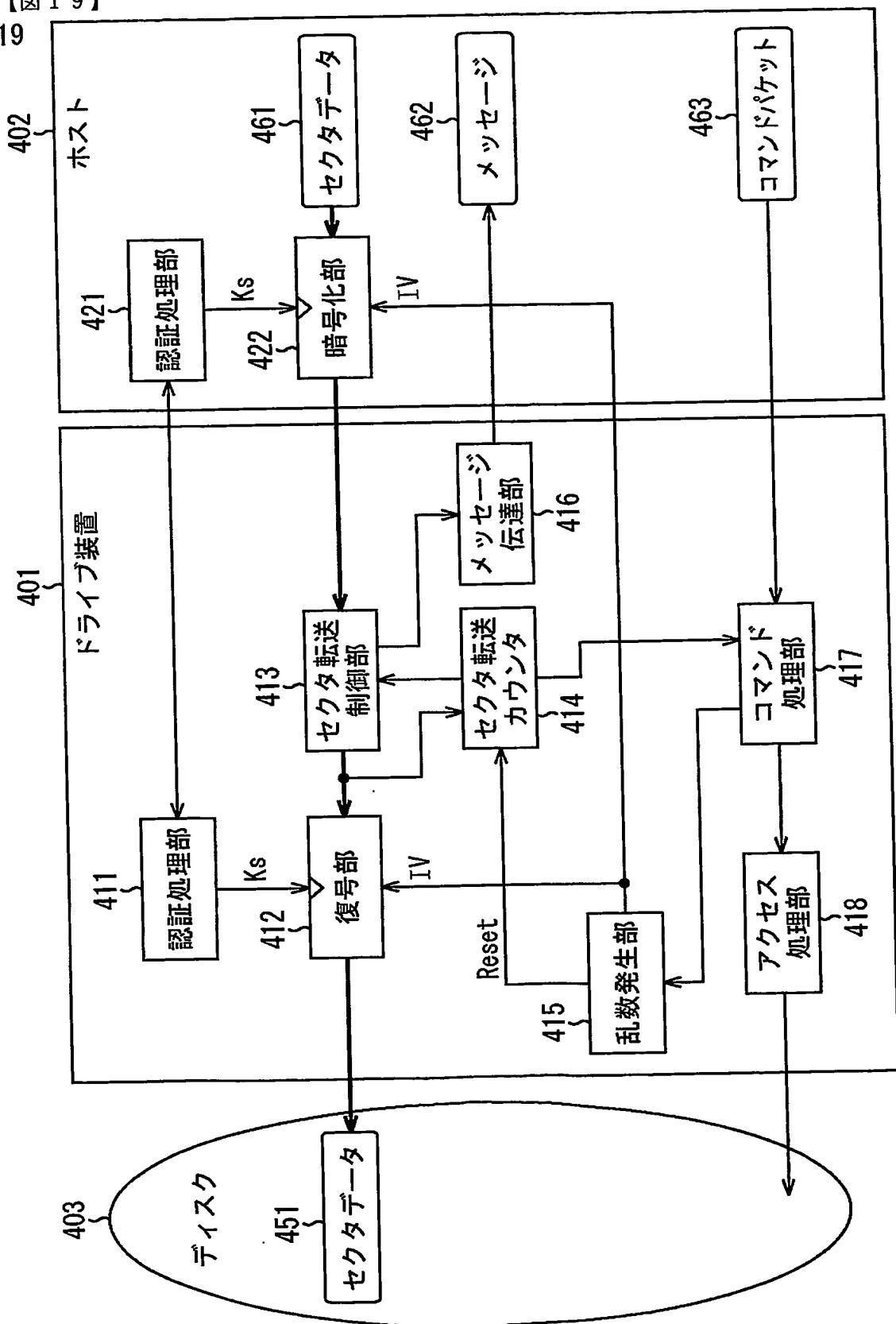
【図17】
図17



【図18】
図18

Byte	7	6	5	4	3	2	1	0
363								
0	Operation Code							
1	LUN(Obsolete)							
2	DP0(0) FUA Reserved RelAdr							
3	Logical Block Address							
4	(MSB)							
5	(LSB)							
6	Transfer Length							
7	(MSB)							
8	(LSB)							
9	Reserved							
10	Streaming							
11	Vendor-Specific Reserved NACA Flag Link							

図19

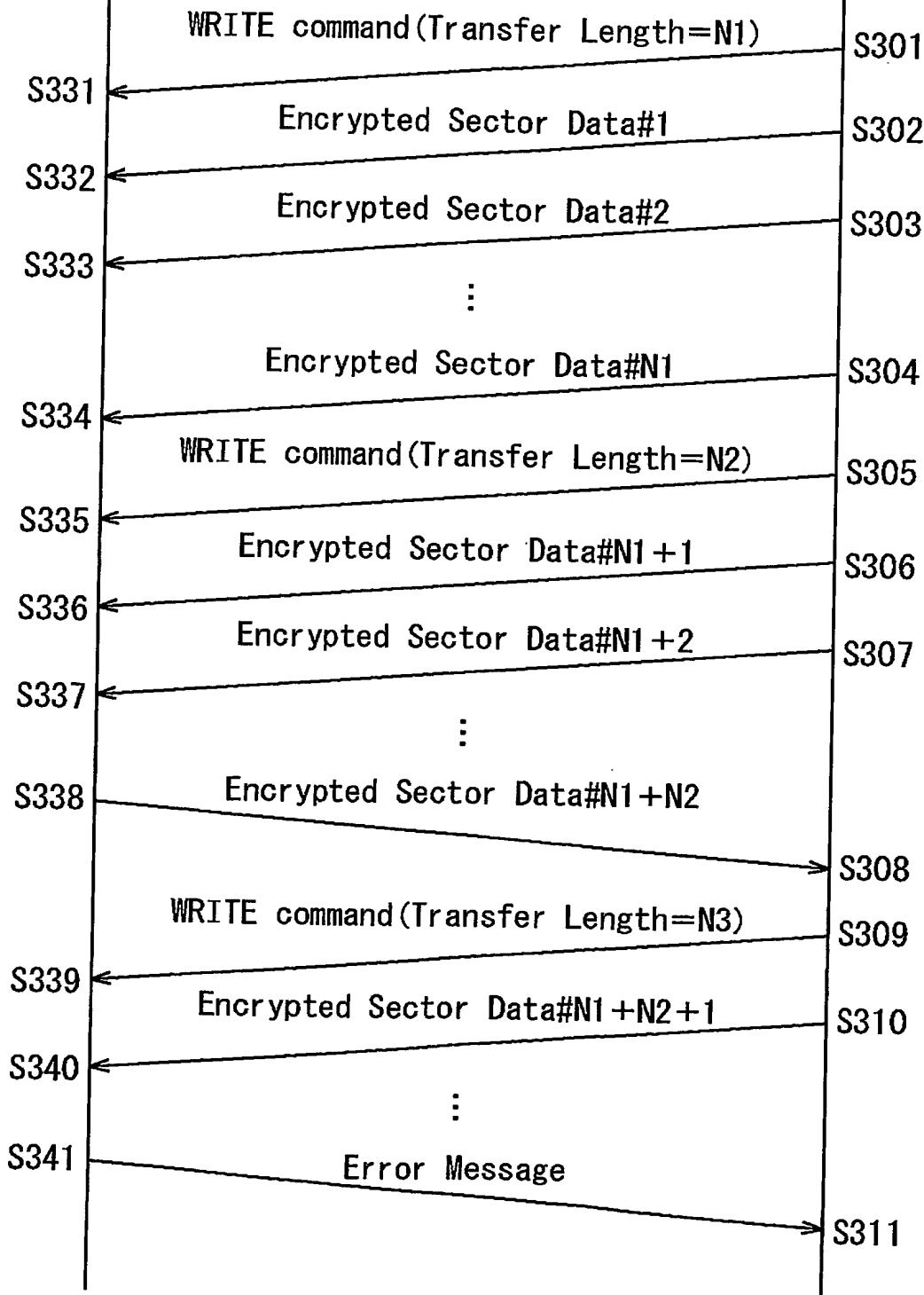


【図20】

図20

ドライブ装置

ホスト



【書類名】要約書

【要約】

【課題】 データの授受をセキュリティを高めた状態で行えるようにする。

【解決手段】 ホストとドライブ装置は、所定のバスで接続されており、そのバスを介してデータの授受を行う。ホストは、ドライブ装置に対して、バス上を介して授受されるデータを暗号化および復号の際に用いられる初期ベクトルIVの発行の要求を定期的に行う。ドライブ装置は、要求があったとき、初期ベクトルIVを生成しホストに供給する。このような処理が定期的に行われなければ、ドライブ装置は、ホストに対するデータの出力を停止する。本発明は、記録媒体に記録されているデータを再生するドライブ装置を有するパーソナルコンピュータに適用することが可能である。

【選択図】図16

特願 2004-004798

出願人履歴情報

識別番号

[000002185]

1. 変更年月日

1990年 8月30日

[変更理由]

新規登録

住 所

東京都品川区北品川6丁目7番35号

氏 名

ソニー株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/000061

International filing date: 06 January 2005 (06.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-004798
Filing date: 09 January 2004 (09.01.2004)

Date of receipt at the International Bureau: 04 February 2005 (04.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse